



**U  
S  
A  
I  
S  
E  
C**

# **LAYER 3 SWITCH EVALUATION PLAN**

**BY  
COMMUNICATION SYSTEMS  
EVALUATION TEAM**

**FEBRUARY 2002**

**DISTRIBUTION A**

**Approved for public release; distribution is unlimited.**

**TECHNOLOGY INTEGRATION CENTER**

**DEPARTMENT OF THE ARMY  
U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND  
FORT HUACHUCA, ARIZONA 85613-5300**

### **DISCLAIMER**

**The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.**

### **CHANGES**

**Refer requests for all changes that affect this document to: USAISEC, ATTN: AMSEL-IE-TI, Fort Huachuca, AZ 85613-5300.**

### **DISPOSITION INSTRUCTIONS**

**Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.**

# LAYER 3 SWITCH EVALUATION PLAN

BY  
COMMUNICATION SYSTEMS EVALUATION TEAM

FEBRUARY 2002

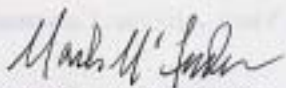
U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND  
TECHNOLOGY INTEGRATION CENTER

## Distribution Statement A

Approved for public release; distribution is unlimited.

## PRODUCT CERTIFICATION

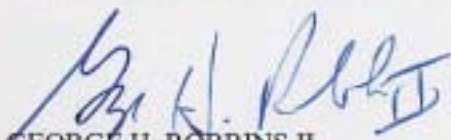
Signatures below indicate that this product does not develop a design or require a formal architectural review and complies with all USAISEC standards.



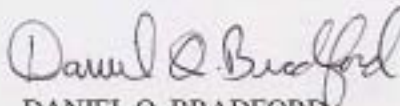
MARK D. MCFADDEN  
Electrical Engineer  
Communication Systems Evaluation Team



MARK H. BEATTIE  
Team Leader  
Communication Systems Evaluation Team



GEORGE H. ROBBINS II  
Group Leader  
Technology Assessment Group



DANIEL Q. BRADFORD  
Director  
Technology Integration Center

## ACKNOWLEDGMENT

The following individuals are acknowledged for their participation in this effort:

Mr. Jeff Bhe; SIGNAL Corporation; 101 Wilcox, Sierra Vista, Arizona; Commercial 520-533-3293, DSN 821-3293.

Mr. Paul Carlson; SIGNAL Corporation; 101 Wilcox, Sierra Vista, Arizona; Commercial 520-533-3455, DSN 821-3455.

Mr. Trace Gunsch; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; Commercial 520-533-2860, DSN 821-2860.

Mr. Jim Hatch; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; Commercial 520-533-3805, DSN 821-3805.

Mr. Darren Haws; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; Commercial 520-533-3921, DSN 821-3921.

Mr. Jim Johnson; U.S. Army Information Systems Engineering Command, Technology Integration Center, ATTN: AMSEL-IE-TI, Fort Huachuca, Arizona; Commercial 520-533-3921, DSN 821-3321.

Mr. John Kuginski; SIGNAL Corporation; 101 Wilcox, Sierra Vista, Arizona; Commercial 520-533-7209, DSN 821-7209.

Mr. Scott Lange; SIGNAL Corporation; 101 Wilcox, Sierra Vista, Arizona; Commercial 520-533-3577, DSN 821-3577.

Mr. Robert Sacha; U.S. Army Information Systems Engineering Command, Infrastructure Systems Engineering Directorate, ATTN: AMSEL-IE-IS, Fort Huachuca, Arizona; Commercial 520-533-2510, DSN 821-2510.

Mr. Tony Schaffer; SIGNAL Corporation; 101 Wilcox, Sierra Vista, Arizona; Commercial 520-533- 3362, DSN 821-3362.

## EXECUTIVE SUMMARY

Product Manager, Defense Data Networks (PM, DNN) tasked the U.S. Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC) to evaluate layer 3 switches to determine if they meet the requirements outlined in *Statement of Requirement for the Common User Installation Transport Network (CUITN)*, Appendix B, *Gigabit Ethernet Data System Specification for CUITN* (CUITN specification), dated 19 July 2001.

This evaluation plan presents the procedures that will be used in TIC labs to perform the layer 3 switch evaluations. Layer 3 switch evaluations are part of on-going TIC support to the CUITN program.

## TABLE OF CONTENTS

	<b>Page</b>
1.0 INTRODUCTION .....	1
1.1 Background.....	1
1.2 Objective.....	1
1.3 Evaluation Overview .....	1
1.4 Evaluation Summary .....	2
1.5 Scoring.....	4
2.0 STANDALONE PERFORMANCE .....	6
2.1 Edge Performance.....	6
2.2 Core Performance .....	14
2.3 Combined Edge/Core Performance .....	24
3.0 SYSTEM FUNCTIONALITY.....	30
3.1 Overview.....	30
3.2 System Functionality Tests.....	31
4.0 NETWORK MANAGEMENT.....	36
4.1 Management Questionnaire .....	36
4.2 Network Management Tests .....	36
5.0 SECURITY .....	43
5.1 Security Requirement Traceability .....	43
5.2 Security Test Methodology .....	43

### Appendices

Appendix A. Standalone Performance Data .....	A-1
Appendix B. System Functionality Data .....	B-1
Appendix C. Network Management Data.....	C-1
Appendix D. Security Data .....	D-1
Appendix E. Features Questionnaire .....	E-1
Appendix F. Vendor Information .....	F-1
Appendix G. SmartBITs Configuration.....	G-1
Appendix H. System Functionality Test Configuration .....	H-1
Glossary. Acronyms and Abbreviations .....	Glossary-1

### Tables

Table 1. Evaluation Summary.....	2
Table 2. Scoring .....	6
Table 3. VLAN Prioritization .....	21
Table 4. IP Address Prioritization.....	21
Table 5. Application Flow Prioritization .....	21
Table A-1. Single Edge Forwarding Results .....	A-1
Table A-2. Single Edge IFG Results .....	A-2
Table A-3. Single Edge Congestion Control Results .....	A-2
Table A-4. Single Edge Error Filtering Results.....	A-2

	<b>Page</b>
Table A-5. Single Edge Address Caching Results .....	A-2
Table A-6. Single Edge Port Mirroring Results .....	A-3
Table A-7. Edge Link Aggregation Results .....	A-3
Table A-8. Edge 8-Port GbE Throughput Results .....	A-3
Table A-9. Core 64-Port Performance Results .....	A-4
Table A-10. Core IFG Results .....	A-6
Table A-11. Core Congestion Control Results .....	A-6
Table A-12. Core Error Filtering Results .....	A-6
Table A-13. Core Address Caching Results .....	A-7
Table A-14. Core Port Mirroring Results .....	A-7
Table A-15. Core Link Aggregation Results .....	A-7
Table A-16. Core Quality of Service Results .....	A-7
Table A-17. Core Multicast Performance Results .....	A-10
Table A-18. Core 10/100 Port Performance Results .....	A-11
Table A-19. Combined Edge/Core Bridging Results .....	A-13
Table A-20. Broadcast Distribution and Leak Results .....	A-14
Table A-21. Edge Routing Results .....	A-14
Table A-22. VLAN Tagging - Bridging and Routing Results .....	A-15
Table A-23. Combined Edge/Core Multicast Performance .....	A-17
Table B-1. FTP Series Results .....	B-1
Table B-2. Overnight Results .....	B-2
Table B-3. Network Recovery Results .....	B-2
Table B-4. Progressive Multicast Results .....	B-3
Table B-5. Multicast Channel Surfing Results .....	B-4
Table B-6. Multicast One-to-Many Results .....	B-4
Table B-7. General Notes on System Testing .....	B-4
Table C-1. Telnet Results .....	C-1
Table C-2. SNMP MIB Walk Results .....	C-1
Table C-3. SNMP SET/GET Requests Results .....	C-1
Table C-4. SNMP Traps Results .....	C-1
Table C-5. SNMP Security Results .....	C-2
Table C-6. Network Element Configuration Results .....	C-2
Table C-7. Port VLAN Identifier Results .....	C-2
Table C-8. Device Performance Monitoring Results .....	C-2
Table C-9. Network VLAN Configuration Results .....	C-3
Table C-10. Management Questionnaire .....	C-3
Table D-1. Audit Results .....	D-1
Table D-2. Configuration Management with Secure Remote Management Results .....	D-1
Table D-3. Product Integrity and Assurance Results .....	D-2
Table D-4. Network Based Attack Detection Results .....	D-3
Table D-5. Access Control Filters Results .....	D-4
Table D-6. Backup and Redundancy Results .....	D-4
Table E-1. Additional Features Support .....	E-1
Table F-1. Device Requirements .....	F-1
	<b>Page</b>

Table F-2. Tests Performed on Each Device .....	F-2
Table G-1. SmartBits Hardware .....	G-2
Table H-1. RTE 201-236 IP Addressing 6-Subnet .....	H-7
Table H-2. RTE 201-236 IP Addressing 6-VLAN .....	H-8
Table H-3. RTE 201-236 IP Addressing 36-Subnet .....	H-9
Table H-4. RTE Multicast Groups .....	H-10

## Figures

Figure 1. Single Edge Forwarding 100 Mbps Configuration .....	7
Figure 2. Single Edge Forwarding 1000 Mbps Configuration .....	7
Figure 3. Single Edge IFG Configuration .....	8
Figure 4. Single Edge Congestion Control Configuration .....	9
Figure 5. Single Edge Error Filtering Configuration .....	10
Figure 6. Single Edge Address Caching Configuration .....	11
Figure 7. Single Edge Port Mirroring Configuration .....	12
Figure 8. Edge Link Aggregation Configuration .....	13
Figure 9. Edge 8-Port GbE Throughput Configuration .....	14
Figure 10. Core 64-Port Performance Configuration .....	15
Figure 11. Core IFG Configuration .....	16
Figure 12. Core Congestion Control Configuration .....	16
Figure 13. Core Error Filtering Configuration .....	17
Figure 14. Core Address Caching Configuration .....	18
Figure 15. Core Port Mirroring Configuration .....	18
Figure 16. Core Link Aggregation Configuration .....	19
Figure 17. Core QoS Configuration .....	20
Figure 18. Core Multicast Performance Configuration .....	22
Figure 19. Core 10/100-Port Performance Configuration .....	24
Figure 20. Bridging Configuration .....	25
Figure 21. Broadcast Distribution and Leak Configuration .....	26
Figure 22. Edge Routing Configuration .....	27
Figure 23. VLAN Tagging – Bridging and Routing Configuration .....	28
Figure 24. Multicast Performance Configuration .....	29
Figure 25. FTP Series Logical Traffic Flow for 6-Subnet .....	31
Figure 26. NMS Configuration .....	37
Figure 27. Network Element Configuration .....	41
Figure 28. Security Lab Network Configuration .....	44
Figure H-1. 6-Subnet Configuration with L2 at Tier 1 .....	H-3
Figure H-2. 6-Subnet Configuration with L3 at Tier 1 .....	H-4
Figure H-3. 6-VLAN Configuration and VLAN Logical Flow .....	H-5
Figure H-4. 6-VLAN Logical Connections .....	H-6



## LAYER 3 SWITCH EVALUATION PLAN

### 1.0 INTRODUCTION

This evaluation plan describes how the U.S. Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC) will evaluate Ethernet layer 3 switches. This is Phase 3 of an ongoing evaluation. Phase 1 explored the current state of the technology, Phase 2 expanded the number of items tested, and Phase 3 clarifies what is expected in each test.

#### 1.1 Background

The Army's Common User Installation Transport Network (CUITN) program, administered by Product Manager, Defense Data Networks (PM, DDN) at Fort Monmouth, New Jersey, and engineered by USAISEC at Fort Huachuca, Arizona, evaluates and fields the backbone infrastructure that provides data communications capability to Army users on continental U.S. (CONUS) installations. The TIC was tasked to evaluate commercial layer 3 switches to determine if they meet the specifications outlined in the *Statement of Requirement for CUITN*, Appendix B, *Gigabit Ethernet Data System Specification for CUITN* (dated 19 July 2001). Core switches have Gigabit Ethernet (GbE) interfaces and edge devices have GbE and Fast Ethernet (FE) interfaces.

#### 1.2 Objective

The objective is to determine if the Ethernet layer 3 switches meet the requirements for possible implementation in the U.S. Army CUITN infrastructure. To meet this objective, the TIC Evaluation Team will answer the following questions:

- a. What are the capabilities of Ethernet switching devices in a standalone environment?
- b. How do Ethernet switching devices inter-operate in a system environment?
- c. What network management capabilities do Ethernet switching devices support?
- d. What security features do the Ethernet switching devices support?

#### 1.3 Evaluation Overview

For this evaluation the devices under test (DUT) will be commercial off-the-shelf (COTS) GbE/FE edge devices and GbE core switches. Edge devices are typically layer 2 switches and may or may not support layer 3 routing. Chassis-based edge devices must support layer 3 in order to be considered as a building switch. Core switches are typically layer 3 switches performing routing functions.

The evaluation consists of the four following categories. Each of these categories is comprised of tests and subtests to meet the evaluation objectives.

- a. Standalone Performance. Both the edge device and core switch are evaluated. These device level tests measure the performance of the standalone device using a SmartBits packet analyzer. Section 2 contains the evaluation procedure for both the edge device and the core switch.
- b. System Functionality. Each device under test is installed in a configuration resembling the CUITN architecture. These system level tests measure the performance of all devices as a complete system. Section 3 contains the system level evaluation procedure.

c. Network Management. Network management capabilities of the Ethernet switching devices are evaluated using the System Functionality test configuration. Section 4 contains the network management evaluation procedure.

d. Security. The core switch and edge device go through a security assessment to determine the security impact when the switch is integrated into the CUITN architecture. Section 5 contains the security evaluation procedure.

Data from each of these four categories is recorded in appendices A through D. In addition to these tests, the Evaluation Team will complete a features questionnaire listing capabilities supported but not verified by this evaluation. See Appendix E for the features questionnaire. Appendix F provides details on device requirements and information to the vendor on related administrative issues. Appendix G provides more details on SmartBits configurations. Appendix H provides more details on the remote terminal emulation (RTE) configuration.

## 1.4 Evaluation Summary

Table 1 lists all of the tests that are performed during the evaluation, along with the priority, a summary of the pass/fail criteria, and data tables.

**Table 1. Evaluation Summary**

Test Ref	Test Name	Priority	Pass/Fail Criteria	Data Table
<b>Edge Performance</b>				
<a href="#">2.1.1</a>	Single Edge Forwarding	1	PASS if throughput is 75% or greater for all packet sizes.	<a href="#">A-1</a>
<a href="#">2.1.2</a>	Single Edge Interframe Gap (IFG)	1	PASS if IFG is 0.96 microseconds or greater for FE and 0.096 or greater for GbE.	<a href="#">A-2</a>
<a href="#">2.1.3</a>	Single Edge Congestion Control	3	FAIL if there is loss on the uncongested port or the loss on the congested port exceeds 33.3%.	<a href="#">A-3</a>
<a href="#">2.1.4</a>	Single Edge Error Filtering	2	FAIL if illegal Ethernet frames are not handled properly.	<a href="#">A-4</a>
<a href="#">2.1.5</a>	Single Edge Address Caching	5	PASS if each port can learn one MAC address.	<a href="#">A-5</a>
<a href="#">2.1.6</a>	Single Edge Port Mirroring	4	PASS if able to mirror ports without dropping packets.	<a href="#">A-6</a>
<a href="#">2.1.7</a>	Edge Link Aggregation (Trunking)	3	FAIL if packets are dropped with 2 gigabits of traffic over 2 GbE links, 10 FE ports are not load shared between 2 GbE ports, or if only one or both fibers of a transmit/receive fiber pair is pulled and the remaining fiber link does not pass all traffic.	<a href="#">A-7</a>
<a href="#">2.1.8</a>	Edge 8-Port GbE Throughput	2	PASS throughput is 75% or greater for all packet sizes.	<a href="#">A-8</a>
<b>Core Performance</b>				
<a href="#">2.2.1</a>	Core 64-Port Performance	1	PASS if throughput is 75% or greater for all packet sizes.	<a href="#">A-9</a>
<a href="#">2.2.2</a>	Core Interframe Gap (IFG)	1	FAIL if IFG less than 0.096 microseconds.	<a href="#">A-10</a>
<a href="#">2.2.3</a>	Core Congestion Control	2	FAIL if there is loss on the uncongested port or the loss on the congested port exceeds 33.3%.	<a href="#">A-11</a>
<a href="#">2.2.4</a>	Core Error Filtering	2	FAIL if illegal Ethernet frames are not handled properly.	<a href="#">A-12</a>

**Table 1. Evaluation Summary (continued)**

Test Ref	Test Name	Priorit y	Pass/Fail Criteria	Data Table
<a href="#">2.2.5</a>	Core Address Caching	5	PASS if each port can learn one MAC addresses.	<a href="#">A-13</a>
<a href="#">2.2.6</a>	Core Port Mirroring	4	PASS if able to mirror ports without dropping packets.	<a href="#">A-14</a>
<a href="#">2.2.7</a>	Core Link Aggregation	3	FAIL if packets are dropped with 8 gigabits of traffic over GbE trunks, if traffic is not distributed between GbE trunks, or if traffic does not redistribute when one trunk is pulled.	<a href="#">A-15</a>
<a href="#">2.2.8</a>	Core Quality of Service (QoS)	4	PASS if core is able to limit low priority traffic in favor of high priority traffic.	<a href="#">A-16</a>
<a href="#">2.2.9</a>	Core Multicast Performance	3	FAIL if the device doesn't support multicast or if packets are dropped with 60% multicast load using 16 groups.	<a href="#">A-17</a>
<a href="#">2.2.10</a>	Core 10/100-Port Performance	3	PASS if throughput is 75% or greater for all packet sizes.	<a href="#">A-18</a>
<b>Combined Edge / Core Performance</b>				
<a href="#">2.3.1</a>	Bridging	2	PASS if throughput is 75% or greater for all packet sizes.	<a href="#">A-19</a>
<a href="#">2.3.2</a>	Broadcast Distribution and Leak	2	FAIL if traffic leaks from one VLAN to another or if traffic is not distributed within it's own VLAN.	<a href="#">A-20</a>
<a href="#">2.3.3</a>	Edge Routing	2	FAIL if edge device does not support layer 3 routing or if edge device interferes with core routing.	<a href="#">A-21</a>
<a href="#">2.3.4</a>	VLAN Tagging - Bridging and Routing	2	FAIL if packets are not properly bridged or routed.	<a href="#">A-22</a>
<a href="#">2.3.5</a>	Multicast Performance	3	FAIL if the device doesn't support multicast or if packets are dropped with 60% multicast load using 16 groups.	<a href="#">A-23</a>
<b>System Functionality</b>				
<a href="#">3.2.1</a>	FTP Series	1	FAIL if users do not pass traffic or if throughput rates vary greatly between users.	<a href="#">B-1</a>
<a href="#">3.2.2</a>	Overnight	1	FAIL if unicast throughput varies by more than 10% from the unicast baseline or if unicast throughput varies by more than 10% from the unicast baseline when multicast traffic is introduced.	<a href="#">B-2</a>
<a href="#">3.2.3</a>	Network Recovery	1	FAIL if edge does not fully recover within 5 minutes or if core does not fully recover within 5 minutes. FAIL if the network cannot re-converge all routing processes and reestablish traffic flows of all types. FAIL if the network cannot recover within 10 seconds when the disrupted system is brought back into normal service.	<a href="#">B-3</a>
<a href="#">3.2.4</a>	Multicast Streams	2	FAIL if multicast cannot join/leave within a reasonable time or cannot provide minimum rate through the core without dropouts while sending 12 MGENs. Dropouts are periods of inactivity lasting longer than 100 milliseconds or inactivity occurring more than one time in any 3-second period.	<a href="#">B-4</a>
<a href="#">3.2.5</a>	Multicast Channel Surfing	3	FAIL if any group or user receives less than 95% of the traffic.	<a href="#">B-5</a>

Test Ref	Test Name	Priority	Pass/Fail Criteria	Data Table
<a href="#">3.2.6</a>	Multicast One-to-Many	3	FAIL if any receiver drops from the group.	<a href="#">B-6</a>

**Table 1. Evaluation Summary (continued)**

Test Ref	Test Name	Priority	Pass/Fail Criteria	Data Table
<b>Network Management</b>				
<a href="#">4.2.1</a>	Telnet - Windows, Solaris, Linux	1	PASS if valid Telnet sessions are established from the specified systems.	<a href="#">C-1</a>
<a href="#">4.2.2</a>	SNMP MIB Walk	2	FAIL if MIB table information is incorrect, or if requests produce errors.	<a href="#">C-2</a>
<a href="#">4.2.3</a>	SNMP SET/GET Requests	1	FAIL if information is not correctly stored and recalled, or if ports do not disable and enable correctly.	<a href="#">C-3</a>
<a href="#">4.2.4</a>	SNMP Traps	2	PASS if traps for link status and at least one type of restart are received for the correct conditions.	<a href="#">C-4</a>
<a href="#">4.2.5</a>	SNMP Security	2	FAIL if device accepts requests from unauthorized stations or accepts SET requests with community strings not granting write permission.	<a href="#">C-5</a>
<a href="#">4.2.6</a>	Network Element Configuration	3	PASS if VLAN is established and is isolated from other ports.	<a href="#">C-6</a>
<a href="#">4.2.7</a>	Port VLAN Identifier	2	FAIL if device allows a second PVID assigned to the same port.	<a href="#">C-7</a>
<a href="#">4.2.8</a>	Device Performance Monitoring	3	PASS if displayed port statistics reflect traffic on the device.	<a href="#">C-8</a>
<a href="#">4.2.9</a>	Network VLAN Configuration	3	PASS if VLAN is established and is isolated from other ports across the network.	<a href="#">C-9</a>
<b>Security</b>				
<a href="#">5.2.1</a>	Audit Capability	2	FAIL if logs cannot be exported, unauthorized user can change audit trail, audit events are not selectable, or rejected connection events are not recorded.	<a href="#">D-1</a>
<a href="#">5.2.2</a>	Configuration Management with Secure Remote Management	1	FAIL if remote management session is not secure, remote administration is unrestricted, or not remotely manageable via web, Telnet and FTP. Secure remote management is required on layer-3 switches and preferred, but not required on layer-2 switches.	<a href="#">D-2</a>
<a href="#">5.2.3</a>	Product Integrity and Assurance	3	FAIL if password aging, password timeout, or minimum 8-character password cannot be set.	<a href="#">D-3</a>
<a href="#">5.2.4</a>	Network Based Attack Detection	3	FAIL if unable to detect attacks or unable to react to attacks.	<a href="#">D-4</a>
<a href="#">5.2.5</a>	Access Control Filters	3	FAIL if unable to associate filters with a specific interface, unable to combine multiple filters on one port, or unable to change rules without dropping.	<a href="#">D-5</a>
<a href="#">5.2.6</a>	Backup and Redundancy	3	FAIL if unable to backup and restore system configuration.	<a href="#">D-6</a>

## 1.5 Scoring

To be recommended for use at CUITN sites each device must pass all priority 1 tests and score above 70% in each of the four test categories. Table 2 shows how the points are awarded to each test based on priority.



**Table 2. Scoring**

<b>Priority</b>	<b>Points</b>
1	10
2	8
3	5
4	2
5	1

The score for each of the four sections is simply the percentage of earned points over total possible points for that section. Scores will be used to compare vendor performance. If test time becomes a problem, the TIC test director may elect not to perform priority 4 and 5 tests. Each device will receive a separate score. One device may fail the evaluation while another device in the same evaluation is approved.

## **2.0 STANDALONE PERFORMANCE**

Device level tests measure the performance of a single device in a standalone environment. A SmartBits packet analyzer is used to measure the functional and performance capabilities. The core and edge devices are evaluated independently and together. Standalone performance is divided into three sections: Edge, Core, and combined Edge/Core. See Appendix A for performance data tables. See Appendix G for more details on SmartBits configurations.

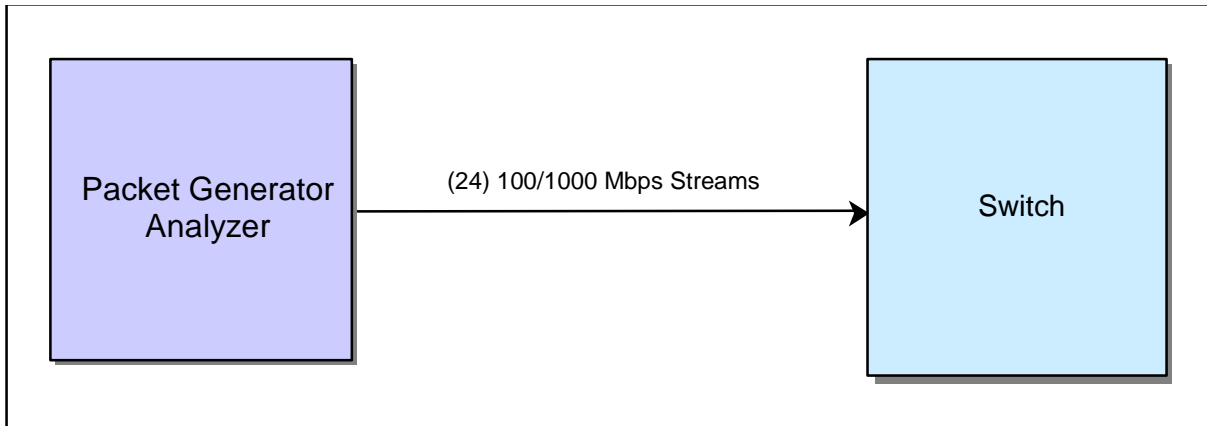
### **2.1 Edge Performance**

The tests in this first section are used to evaluate the edge device. Tests are performed on a single edge device or two edge devices back-to-back.

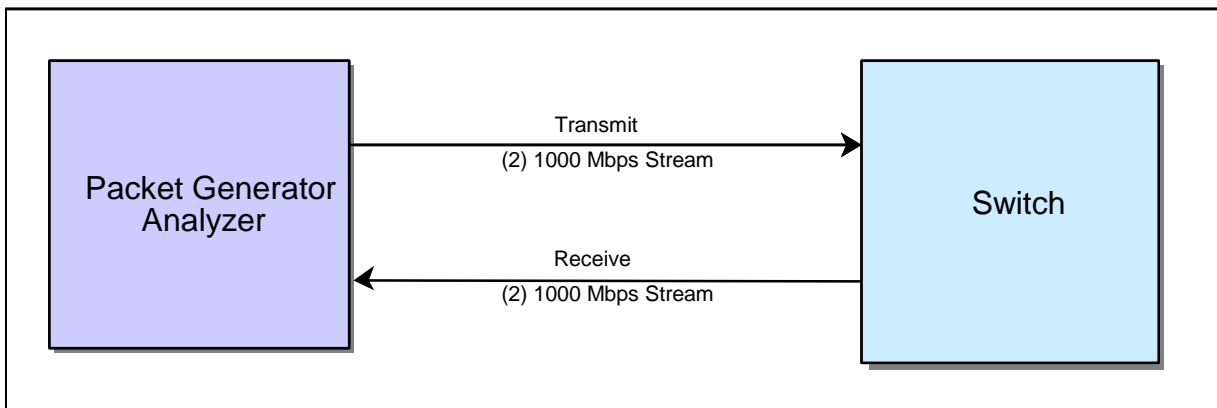
#### **2.1.1 Single Edge Forwarding**

a. **Objective.** Test objective is to measure the performance characteristics of the edge device while forwarding layer 2 traffic.

b. **Configuration.** Figure 1 shows the Single Edge Forwarding 100 megabits per second (Mbps) test configuration. SmartBits is connected to the edge device with twenty-four 100-Mbps streams. Figure 2 shows the Single Edge Forwarding 1000 Mbps test configuration. SmartBits is connected to the edge device with two 1000-Mbps streams.



**Figure 1. Single Edge Forwarding 100 Mbps Configuration**



**Figure 2. Single Edge Forwarding 1000 Mbps Configuration**

**c. Procedure.**

(1) Configure the test analyzer to transmit 24 full-duplex 100-Mbps streams to the edge device.

(2) Use SmartFlow to perform the Throughput and Jumbo tests in a full mesh mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.

(3) Repeat this test using two GbE ports.

(4) Repeat this test transmitting from 10 full-duplex 100-Mbps ports to one GbE port and from one GbE port to 10 full-duplex 100-Mbps ports.

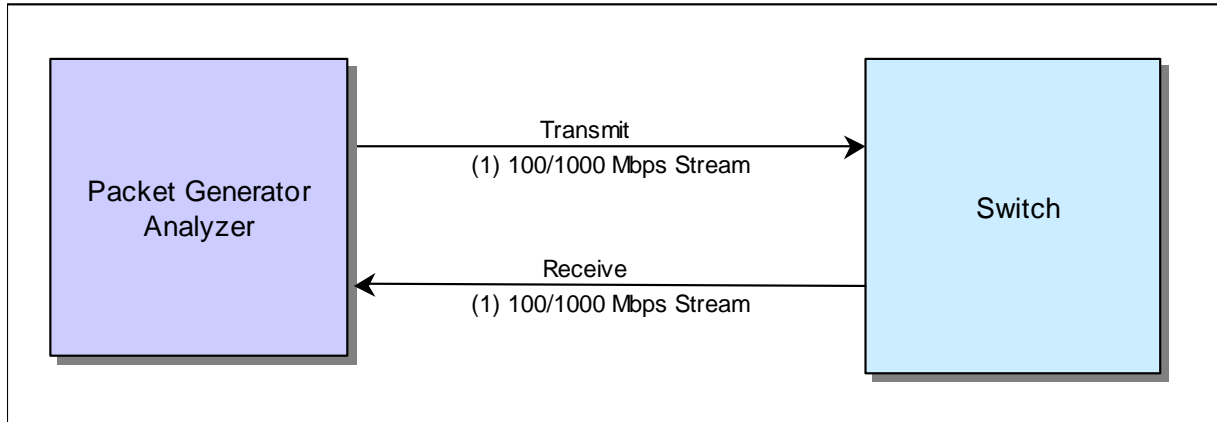
(5) Record results in [Table A-1](#).

(6) PASS if throughput is 75% or greater for all packet sizes.

**2.1.2 Single Edge Interframe Gap (IFG)**

a. **Objective.** Test objective is to measure the minimum Ethernet IFG of an edge device's 100-Mbps and 1000-Mbps interfaces.

b. **Configuration.** Figure 3 shows the Single Edge IFG test configuration. SmartBits is first connected to an edge device with two 100-Mbps streams and then with two 1000-Mbps streams.



**Figure 3. Single Edge IFG Configuration**

c. **Procedure.**

(1) Use the Advanced Switch Test (AST) IFG test on both 100-Mbps and 1000-Mbps ports.

(2) Record results in [Table A-2](#).

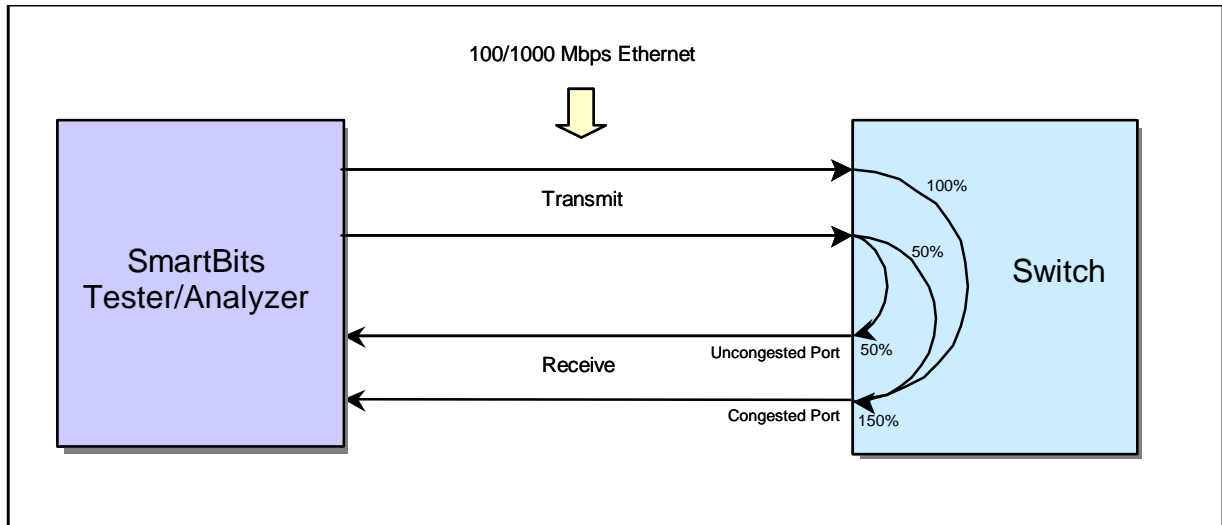
(3) PASS if IFG is 0.96 microseconds or greater for FE and 0.096 or greater for GbE.

### 2.1.3 Single Edge Congestion Control

a. **Objective.** Test objective is to measure an edge device's ability to send pause frames to control SmartBits' transmit port when congestion occurs on 100-Mbps and 1000-Mbps ports.

b. **Configuration.** Figure 4 shows the Single Edge Congestion Control test configuration. There are two configurations. In the first configuration the packet analyzer is connected to the edge device with two 100-Mbps transmit streams and two 100-Mbps receive streams. In the second configuration the packet analyzer is connected to the edge device with two transmit streams (100 Mbps and 1000 Mbps) and two receive streams (100 Mbps and 1000 Mbps).





**Figure 4. Single Edge Congestion Control Configuration**

**c. Procedure.**

(1) Connect four 100-Mbps full-duplex streams from SmartBits to the edge device. Use the AST II Congestion Control test and transmit 64-byte packets. Direct one stream at two different receive ports on the switch. These receive ports are known as the “uncongested port” and the “congested port”.

(2) One stream is evenly distributed between the two receive ports with a 50% load to each. The other transmit stream is a 100% load directed at the congested port. Since the congested port is over-subscribed by 50%, the switch should delay the delivery of packets to the congested port by sending pause frames to the transmitting SmartBits ports. Verify pause frames are detected by SmartBits.

(3) Repeat this test with two 100-Mbps streams and two 1000-Mbps streams to the edge device. The 100-Mbps stream is evenly distributed between the two receive ports with a 50% load to each. The 1000-Mbps transmit stream is a 100% load directed at the congested port. Since the congested port is over-subscribed by 50%, the switch should delay the delivery of packets to the congested port by sending pause frames to the transmitting SmartBits ports. Verify pause frames are detected by SmartBits.

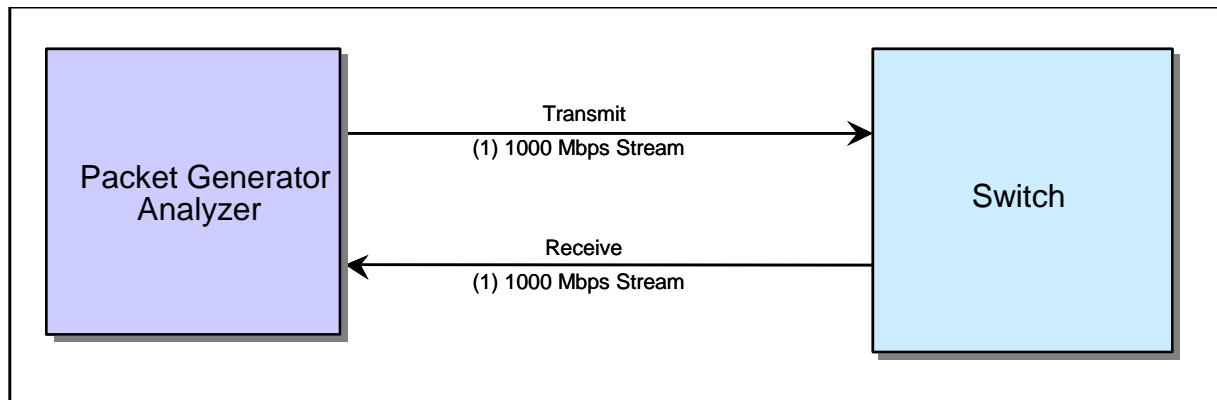
(4) Record results in [Table A-3](#).

(5) FAIL if there is loss on the uncongested port or the loss on the congested port exceeds 33.3%.

**2.1.4 Single Edge Error Filtering**

a. **Objective.** Test objective is to determine the capability of the edge device to filter illegal Ethernet frames.

b. **Configuration.** Figure 5 shows the Single Edge Error Filtering test configuration. There are two configurations. In the first configuration SmartBits is connected to the edge device with two 100-Mbps streams. In the second configuration SmartBits is connected to the edge device with two 1000-Mbps streams.



**Figure 5. Single Edge Error Filtering Configuration**

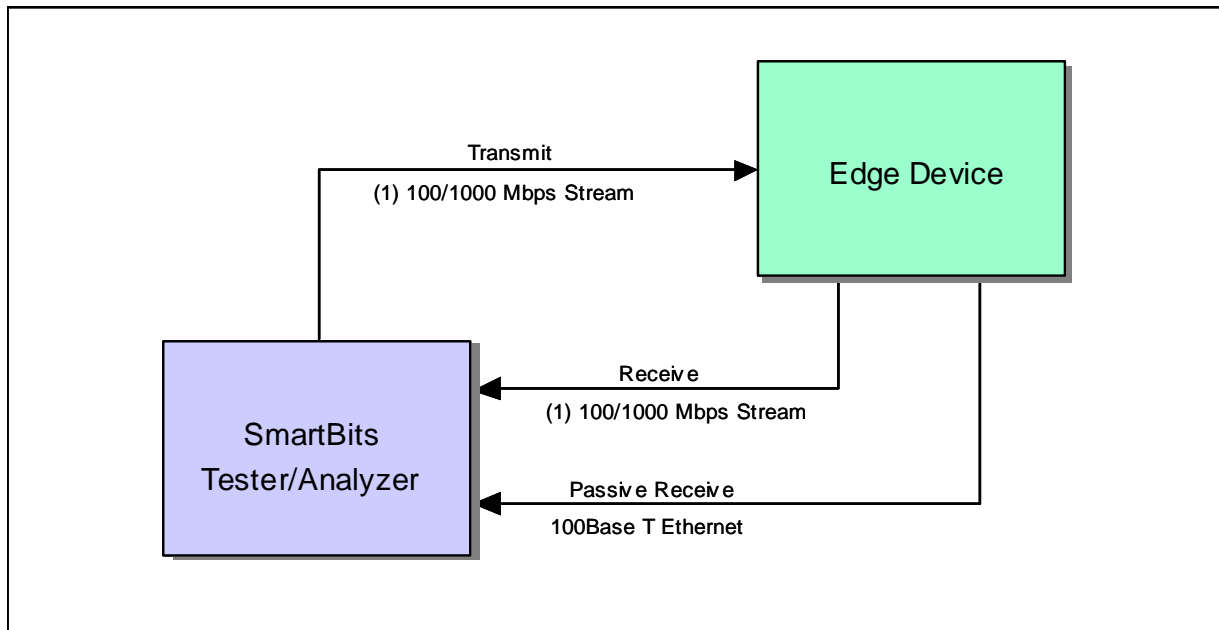
**c. Procedure.**

- (1) Connect SmartBits to the edge device with two 100-Mbps streams.
- (2) Use the AST II Error Filtering test to subject the edge device to the following six illegal frame conditions:
  - (a) Cyclic Redundancy Check (CRC) error
  - (b) Alignment error
  - (c) Dribble Bit
  - (d) Undersize
  - (e) Oversize
  - (f) Virtual local area network (VLAN) oversize
- (3) Record results in [Table A-4](#).
- (4) FAIL if illegal Ethernet frames are not handled properly.

### **2.1.5 Single Edge Address Caching**

a. **Objective.** Test objective is to measure MAC address caching capacity of the edge device on a port-by-port basis.

b. **Configuration.** Figure 6 shows the Single Edge Address Caching test configuration. There are two configurations. In the first configuration, SmartBits is connected to the edge device with two 100-Mbps streams and one 100-Mbps passive receiver. In the second configuration SmartBits is connected to the edge device with two 1000-Mbps streams and one 100-Mbps passive receiver.



**Figure 6. Single Edge Address Caching Configuration**

**c. Procedure.**

(1) Use the AST II Address Caching test to transmit a varying number of unique MAC addresses at 10,000 frames per second (fps) and at line rate. The learning port will transmit the learned addresses back to the test port. Any unlearned addresses are flooded to all ports. The passive receiver will record any flooded packets.

(2) Set the edge device MAC aging time to 30 seconds, if possible, otherwise the lowest, non-zero aging time should be used. Set SmartBits MAC aging time to the switch's minimum plus 3 seconds.

(3) Perform this test for the 100-Mbps and 1000-Mbps ports.

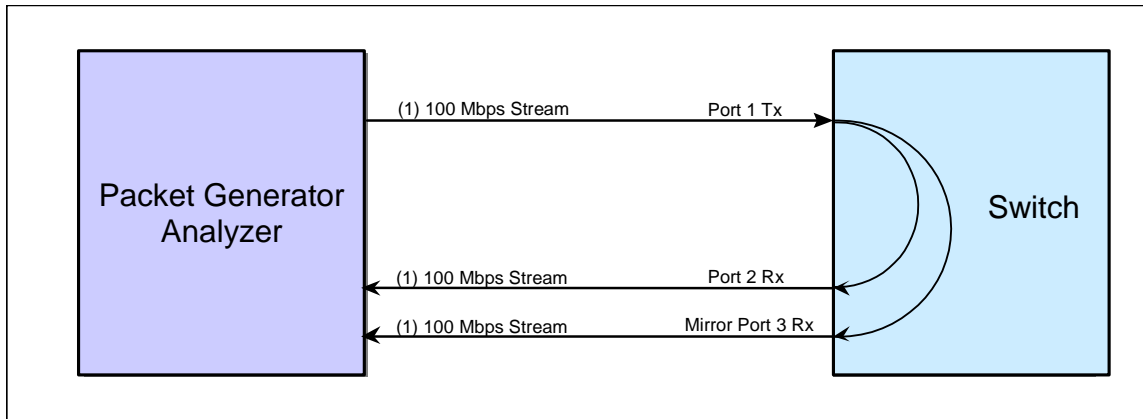
(4) Record results in [Table A-5](#).

(5) PASS if each port can learn one MAC address.

**2.1.6 Single Edge Port Mirroring**

a. **Objective.** Test objective is to verify edge device's ability to mirror traffic to another port.

b. **Configuration.** Figure 7 shows the Single Edge Port Mirroring test configuration. SmartBits is connected to the edge device with three 100-Mbps streams. Port 1 transmits to port 2 and the data stream is mirrored to port 3.



**Figure 7. Single Edge Port Mirroring Configuration**

**c. Procedure.**

(1) Connect SmartBits to the edge device with three 100-Mbps streams. Configure two VLANs and put ports 1 and 2 into VLAN 1 and port 3 into VLAN 2. Configure port 3 to mirror port 1.

(2) Use SmartWindow to transmit a single burst of 10,000 layer 2 frames from port 1 to port 2.

(3) Monitor port 3 to determine whether packets transmitted from port 1 to port 2 are mirrored to port 3.

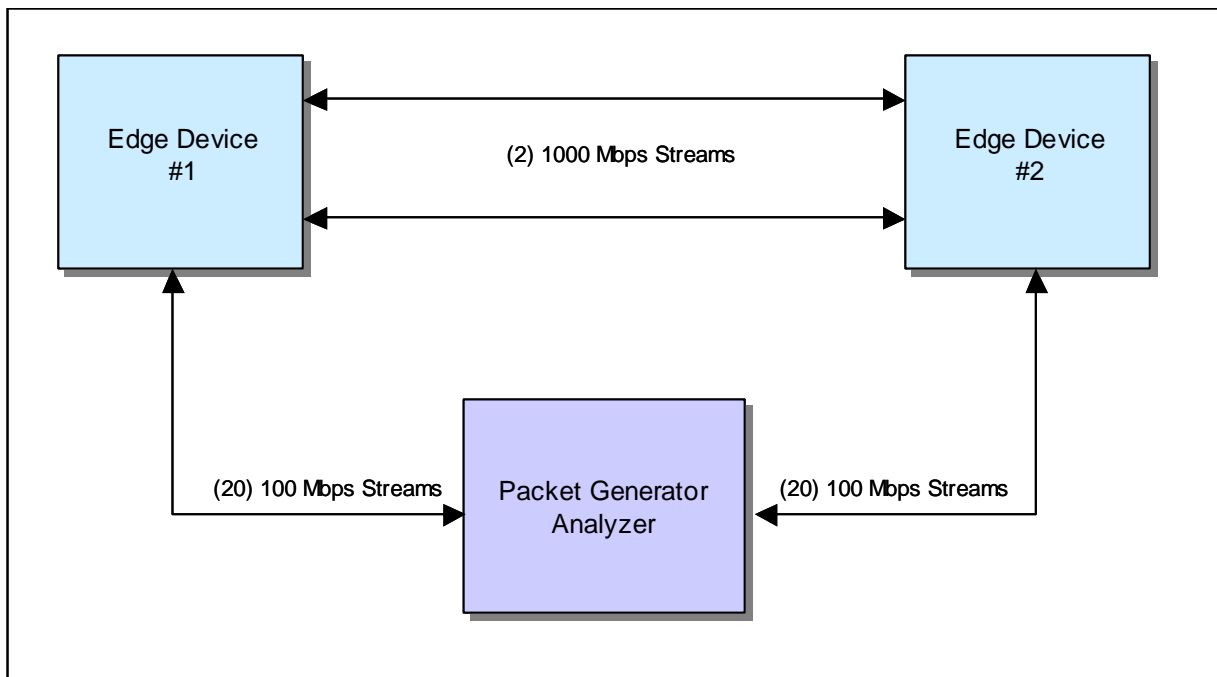
(4) Record results in [Table A-6](#).

(5) PASS if able to mirror ports without dropping packets.

**2.1.7 Edge Link Aggregation (Trunking)**

a. **Objective.** Test objective is to verify the edge device can properly forward traffic across two 1000-Mbps interfaces using link aggregation or load balancing per Institute for Electrical and Electronics Engineers (IEEE) 802.3ad.

b. **Configuration.** Figure 8 shows the Edge Link Aggregation test configuration. There are two configurations. In the first configuration SmartBits is connected to both edge devices using twenty 100-Mbps streams. In the second configuration, SmartBits is connected to both edge devices using ten 100-Mbps streams. The two edge devices are connected with two 1000-Mbps streams and configured for load sharing or link aggregation.



**Figure 8. Edge Link Aggregation Configuration**

**c. Procedure.**

(1) Connect SmartBits to both edge devices using twenty 100-Mbps streams. Connect the two edge devices with two 1000-Mbps streams. Configure the edge devices for load sharing or link aggregation (trunking). Record what method vendor uses for load sharing. Use SmartFlow to generate traffic.

(2) To verify link aggregation or load sharing, monitor the switch MAC tables to see if the traffic is evenly distributed across both ports.

(3) Connect SmartBits to both edge devices using ten 100-Mbps streams.

(4) To verify redundancy, pull the transmit fiber one at a time on each of the GbE links and verify the alternate/secondary link covers for the loss of the first.

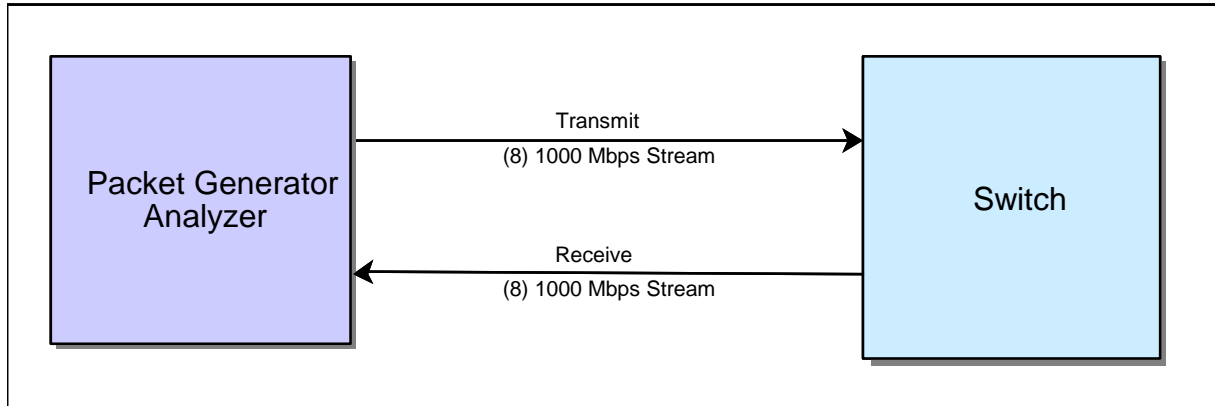
(5) Record results in [Table A-7](#).

(6) FAIL if packets are dropped with 2 gigabits of traffic over two GbE links, ten FE ports are not load shared between two GbE ports, or only one or both fibers of a transmit/receive fiber pair is pulled and the remaining fiber link does not pass all traffic.

### **2.1.8 Edge 8-Port GbE Throughput**

a. **Objective.** Test objective is to measure the throughput of the building switch while forwarding layer 2 traffic and while routing layer 3 traffic.

b. **Configuration.** Figure 9 shows the 8-Port GbE Throughput test configuration. SmartBits is connected to the edge device with eight 1000-Mbps streams.



**Figure 9. Edge 8-Port GbE Throughput Configuration**

**c. Procedure.**

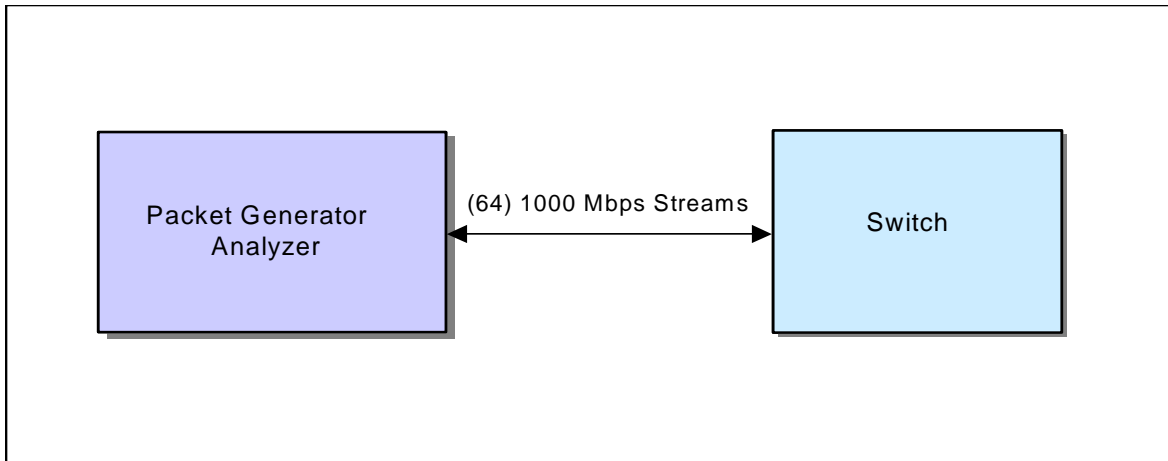
- (1) Configure SmartBits to transmit eight full-duplex 1000-Mbps streams to the edge device. Configure the switch for layer 2 forwarding.
- (2) Use SmartFlow to perform the Throughput and Jumbo tests in a full mesh mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.
- (3) Configure the switch for layer 3 routing and repeat this test.
- (4) Record results in [Table A-8](#).
- (5) PASS if throughput is 75% or greater for all packet sizes.

## 2.2 Core Performance

The tests in this second performance section are used to evaluate the core switch. Core performance testing measures the core switch's capabilities and performance in a standalone environment. All of these tests are performed only on the switch, and many are duplicated tests from the edge performance section of this evaluation plan. See Appendix G for more details on SmartBits configurations.

### 2.2.1 Core 64-Port Performance

- a. **Objective.** Test objective is to measure the performance of the core switch when forwarding and routing traffic between sixty-four 1000-Mbps interfaces.
- b. **Configuration.** Figure 10 shows the Core 64-Port Performance test configuration. SmartBits is connected to the core switch with sixty-four 1000-Mbps streams using multimode fiber.



**Figure 10. Core 64-Port Performance Configuration**

**c. Procedure.**

(1) Connect SmartBits to the core switch with sixty-four 1000-Mbps streams. Configure SmartBits using the Internet Protocol (IP) addresses specified in Appendix G. Use SmartFlow to perform the Throughput and Jumbo tests in a full mesh mode. The four subtests are Forwarding, Routing, Routing with an Access Control List (ACL), and Routing with VLAN tags.

(a) Forwarding. Configure SmartFlow to transmit traffic on a single VLAN. Measure performance for port pairs and full mesh.

(b) Routing. Configure SmartFlow to transmit traffic on 64 subnets. Verify the switch correctly routes IP traffic between the subnets. Measure performance for port pairs and full mesh.

(c) Routing with an ACL. Configure SmartFlow to transmit traffic on 64 subnets. Apply a 1000-line ACL to the core switch. Note maximum ACL capacity. Measure performance only for full mesh.

(d) Routing with VLAN tags. Configure SmartFlow to transmit traffic on 64 VLANs with 802.1Q VLAN tags. Assign each VLAN its own subnet. Verify the switch correctly routes IP traffic between VLANs/subnets. Measure performance only for full mesh.

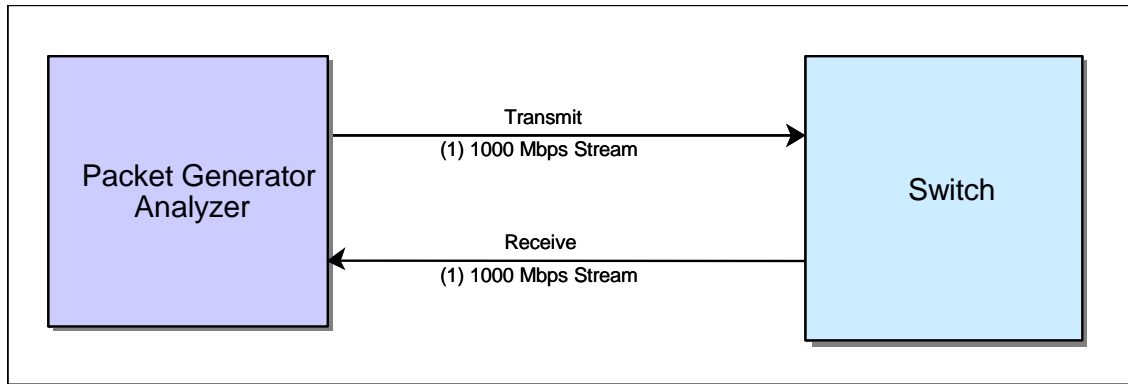
(2) Record results in [Table A-9](#).

(3) PASS if throughput is 75% or greater for all packet sizes.

**2.2.2 Core IFG**

a. **Objective.** Test objective is to measure the minimum Ethernet Interframe Gap (IFG) of the core switch's 1000-Mbps interface.

b. **Configuration.** Figure 11 shows the Core IFG test configuration. SmartBits is connected to the core switch with two 1000-Mbps streams.



**Figure 11. Core IFG Configuration**

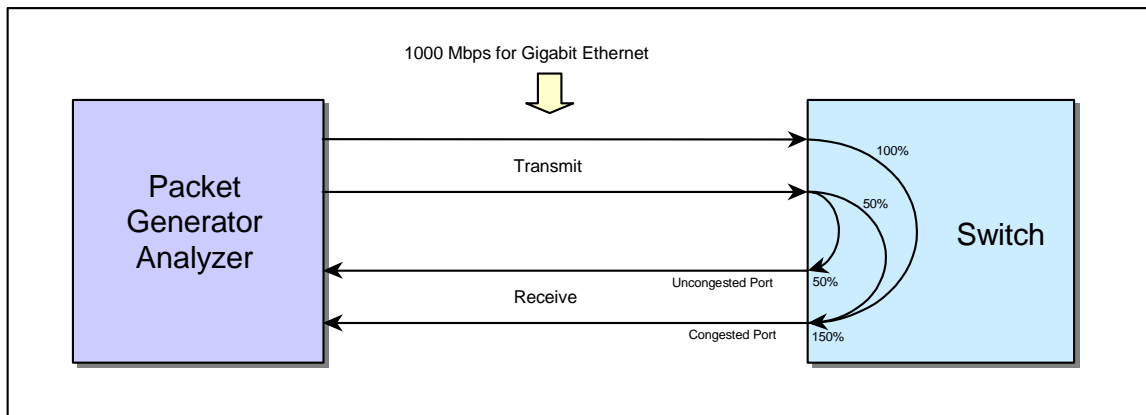
**c. Procedure.**

- (1) Use the AST IFG test on the 1000-Mbps stream of traffic.
- (2) Record results in [Table A-10](#).
- (3) FAIL if IFG is less than 0.096 microseconds.

### 2.2.3 Core Congestion Control

a. **Objective.** Test objective is to measure a core switch's ability to send pause frames to control SmartBits' transmit port when congestion occurs on the 1000-Mbps ports.

b. **Configuration.** Figure 12 shows the Core Congestion Control test configuration. SmartBits is connected to the core switch with two 1000-Mbps transmit streams and two 1000-Mbps receive streams.



**Figure 12. Core Congestion Control Configuration**

**c. Procedure.**

(1) Connect four 1000-Mbps streams from SmartBits to the core switch. Disable flow control on the switch. Use the AST II Congestion Control test and transmit 64-byte packets. Direct one stream at two different receive ports on the switch. These receive ports are known as the uncongested port and the congested port.

(2) One stream is evenly distributed between the two receive ports with a 50% load to each. The other transmit stream is a 100% load directed at the congested port. Since the congested port is over-subscribed by 50%, the switch should delay the delivery of packets to



the congested port by sending pause frames to the transmitting SmartBits ports. Verify pause frames are detected by SmartBits.

(3) Enable flow control on the switch and repeat the test.

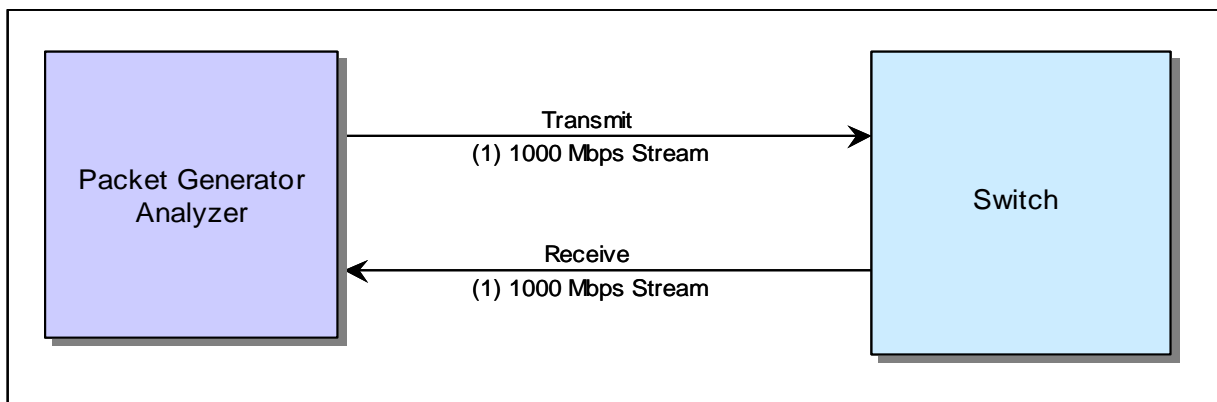
(4) Record results in [Table A-11](#).

(5) FAIL if there is loss on the uncongested port or the loss on the congested port exceeds 33.3%.

#### 2.2.4 Core Error Filtering

a. **Objective.** Test objective is to determine the capability of the core switch to filter illegal Ethernet frames.

b. **Configuration.** Figure 13 shows the Core Error Filtering test configuration. SmartBits is connected to the core switch with two 1000-Mbps streams; one transmit and one receive.



**Figure 13. Core Error Filtering Configuration**

c. **Procedure.**

(1) Connect SmartBits to the core switch with one 1000-Mbps transmit stream and one 1000-Mbps receive stream.

(2) Use the AST II Error Filtering test to subject the edge device to the following four illegal frame conditions:

- (a) Cyclic redundancy code (CRC) errors
- (b) Undersize
- (c) Oversize
- (d) VLAN oversize

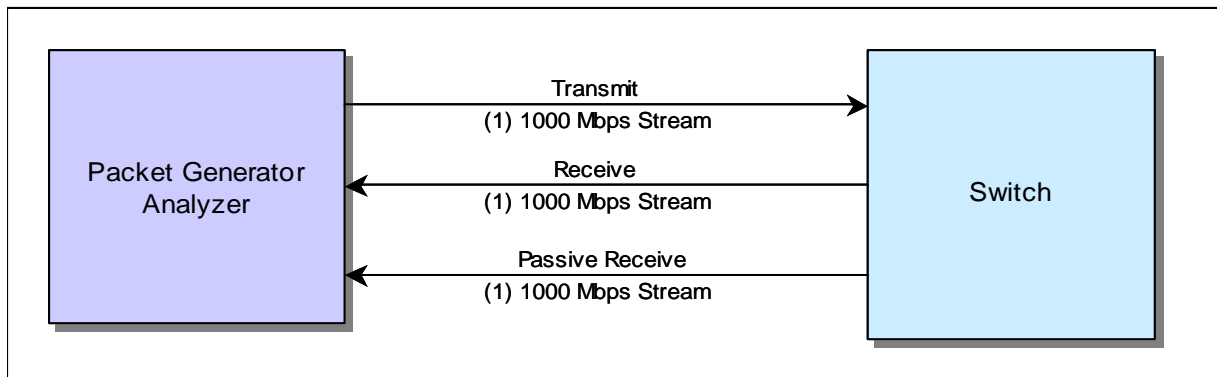
(3) Record results in [Table A-12](#).

(4) FAIL if illegal Ethernet frames are not handled properly.

#### 2.2.5 Core Address Caching

a. **Objective.** Test objective is to measure MAC address caching capacity of the core switch on a port-by-port basis.

b. **Configuration.** Figure 14 shows the Core Address Caching test configuration. SmartBits is connected to the core switch with two 1000-Mbps streams and one 1000-Mbps passive receiver.



**Figure 14. Core Address Caching Configuration**

c. **Procedure.**

(1) Use the AST II Address Caching test to transmit a varying number of unique MAC addresses at 10,000 fps and at line rate. The learning port will transmit the learned addresses back to the test port. Any unlearned addresses are flooded to all ports. The passive receiver will record any flooded packets.

(2) Set the core switch MAC aging time to 30 seconds, if possible, otherwise the lowest, non-zero aging time should be used. Set SmartBits MAC aging time to the switch's minimum plus 3 seconds.

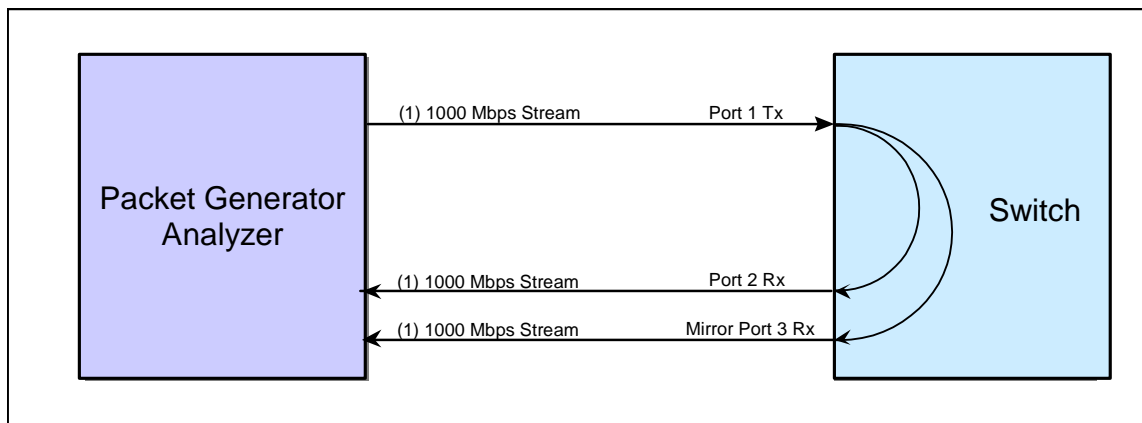
(3) Record results in [Table A-13](#).

(4) PASS if each port can learn one MAC addresses.

## 2.2.6 Core Port Mirroring

a. **Objective.** Test objective is to verify the core switch's ability to mirror traffic to another port.

b. **Configuration.** Figure 15 shows the Core Port Mirroring test configuration. SmartBits is connected to the core switch with three 1000-Mbps streams. Port 1 transmits to port 2 and the data stream is mirrored to port 3.



**Figure 15. Core Port Mirroring Configuration**

**c. Procedure.**

(1) Connect SmartBits to the core switch with three 1000-Mbps streams. Configure two VLANs and put ports 1 and 2 into VLAN 1 and port 3 into VLAN 2. Configure port 3 to mirror port 1.

(2) Use SmartWindow to transmit a single burst of 10,000 layer 2 frames from port 1 to port 2.

(3) Monitor port 3 to determine whether packets transmitted from port 1 to port 2 are mirrored to port 3.

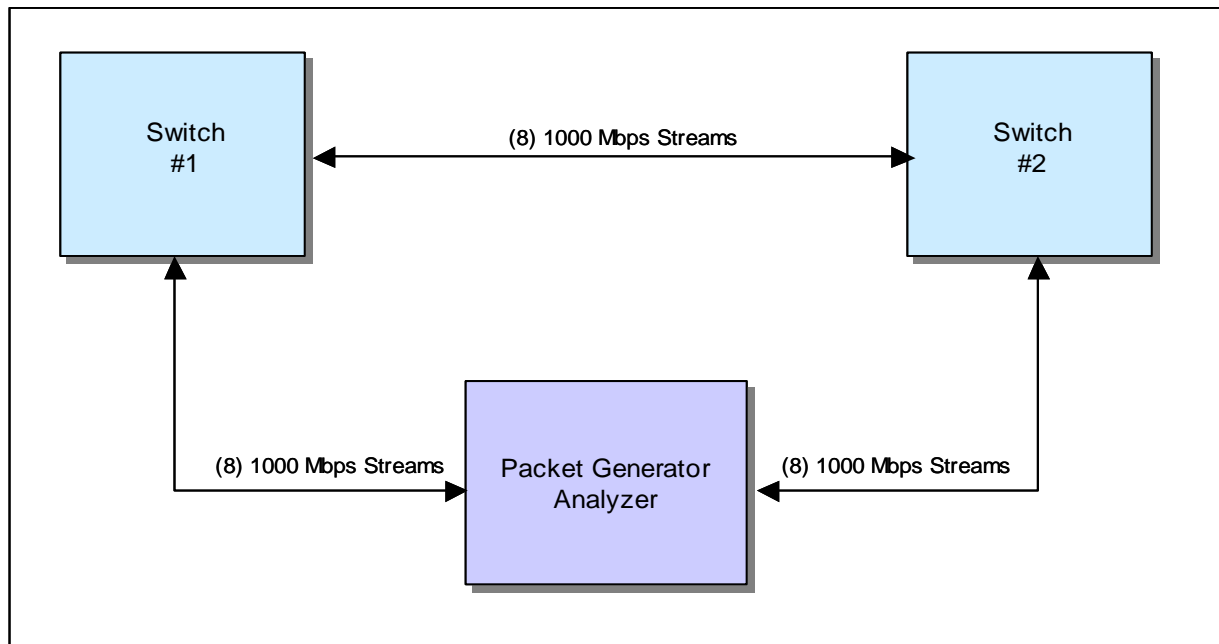
(4) Record results in [Table A-14](#).

(5) PASS if able to mirror ports without dropping packets.

### 2.2.7 Core Link Aggregation

a. **Objective.** Test objective is to determine the capability of the core switch to properly implement link aggregation per IEEE 802.3ad.

b. **Configuration.** Figure 16 shows the Core Link Aggregation test configuration. SmartBits is connected to each of two core switches with eight 1000-Mbps streams. The core switches are connected to each other with eight 1000-Mbps streams.



**Figure 16. Core Link Aggregation Configuration**

**c. Procedure.**

(1) Connect SmartBits to two core switches with eight 1000-Mbps streams. Connect the two core switches to each other with eight 1000-Mbps streams. Configure the core switches for load sharing or link aggregation.

(2) Use SmartFlow to generate traffic. Ramp up from 10% to 100% load.

(3) Monitor the switch MAC tables and note how the traffic is distributed across the trunks.

(4) With a 75% load, pull the fiber pair on one of the GbE trunks and verify traffic is redistributed among the remaining trunks. Reconnect the fiber pair, verify the trunk is re-established, and verify the traffic is again redistributed. Repeat for the remaining seven ports.

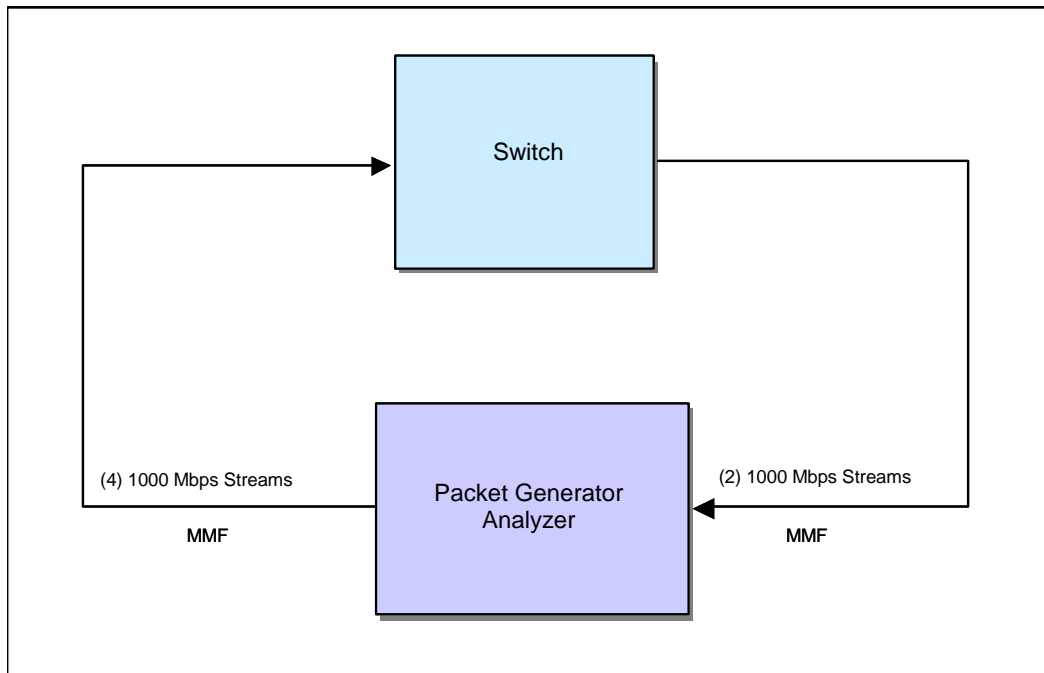
(5) Record results in [Table A-15](#).

(6) FAIL if packets are dropped with 8 gigabits of traffic over GbE trunks, traffic is not distributed between GbE trunks, or traffic does not redistribute when one trunk is pulled.

### 2.2.8 Core Quality of Service

a. **Objective.** Test objective is to measure the core switch's ability to classify and queue traffic using 802.1P precedence bits.

b. **Configuration.** Figure 17 shows the Core Quality of Service (QoS) test configuration. SmartBits is connected to the core switch with four transmit and two receive streams providing a 2:1 over-subscription.



**Figure 17. Core QoS Configuration**

c. **Procedure.**

(1) Connect SmartBits to the core switch with four 1000-Mbps transmit streams and two 1000-Mbps receive streams.

(2) Use SmartFlow to perform the Jumbo tests using a 128-byte frame size. The following three QoS functional areas are tested.

(a) VLAN Prioritization. Use SmartFlow to configure four different traffic groups. Assign each group to a separate VLAN. Configure the core switch to prioritize traffic based on VLAN tags. Table 3 shows the VLAN priorities to use for the four groups:

**Table 3. VLAN Prioritization**

Group	Priority
VOIP / VLAN 1	7
TELNET / VLAN 2	5
FTP / VLAN 3	3
HTTP / VLAN 4	1

(b) IP Address Prioritization. Use SmartFlow to configure four different traffic groups. Assign a different IP address to each group on each port. Configure the core switch to prioritize traffic based on IP address. Table 4 shows the IP address priorities to use for the four groups:

**Table 4. IP Address Prioritization**

Group	Priority
VOIP / IP Group1	7
TELNET / IP Group 2	5
FTP / IP Group 3	3
HTTP / IP Group 4	1

(c) Application Flow Prioritization. Use SmartFlow to configure four different traffic groups. Assign each group to a different application. Configure the core switch to prioritize traffic based on application. Table 5 shows the application flow priorities to use for the four groups:

**Table 5. Application Flow Prioritization**

Group	Priority
VOIP	7
TELNET	5
FTP	3
HTTP	1

(3) Verify the core switch supports 802.1P precedence by observing packet loss on lower priority traffic and no packet loss on higher priority packets.

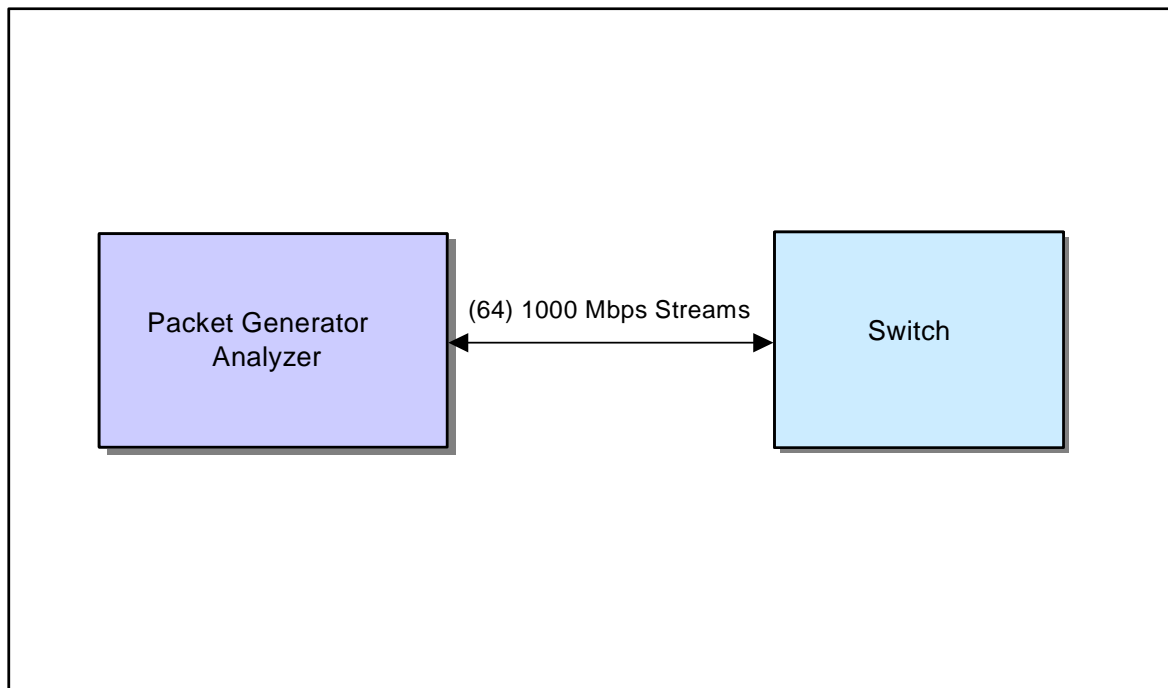
(4) Record results in [Table A-16](#).

(5) PASS if core is able to limit low priority traffic in favor of high priority traffic.

### 2.2.9 Core Multicast Performance

a. **Objective.** Test objective is to measure core switch multicast performance using mixtures of unicast and multicast traffic and to determine the maximum number of multicast groups supported.

b. **Configuration.** Figure 18 shows the Core Multicast Performance test configuration. SmartBits is connected to the core switch with sixty-four 1000-Mbps transmit and receive streams.



**Figure 18. Core Multicast Performance Configuration**

c. **Procedure.**

(1) Enable Internet Group Management Protocol (IGMP) snooping, open shortest path first (OSPF), and Protocol Independent Multicast (PIM) routing protocols on the core switch. Use Distance Vector Multicast Routing Protocol (DVMRP) if PIM is not supported.

(2) Configure the following SmartMulticastIP general settings:

- |  |                               |
|--|-------------------------------|
| (a) Duration                               | 30 seconds                    |
| (b) Number of trials                       | 1                             |
| (c) Transmit delay after joins             | 2                             |
| (d) Delay after transmission               | 2                             |
| (e) Custom frame sizes                     | 64, 256, 1408, and 1518 bytes |
| (f) Group membership verification attempts | 2                             |
| (g) Verify after each join                 | checked                       |
| (h) ARPs or learning frames attempts       | 5                             |

(3) Use SmartMulticastIP to perform each of the four following subtests:

(a) **Multicast Traffic.** Configure SmartMulticastIP for multicast only traffic. Configure 16 concurrent traffic groups with one transmitter, two receivers, and one monitor per group. Configure one receiver on the same blade as the transmitter; configure the other receiver and monitor on a different blade than the transmitter. Configure each stream

transmitted by SmartBits in a separate subnet. Configure SmartMulticastIP in step mode with the following settings:

- Group count 1
- Initial rate 40%
- Maximum rate 100%
- Step rate 20%

(b) Multicast and Unicast Traffic. Configure SmartMulticastIP for multicast and unicast traffic. Use the same 16 groups during the multicast traffic subtest, but gradually introduce unicast traffic at the same rate as the multicast traffic. Configure SmartMulticastIP in step mode with the following settings:

- Group count 1
- Initial rate 10%
- Maximum rate 50%
- Step rate 10%

(c) Scaled Group Forwarding. Configure SmartMulticastIP for Scaled Group forwarding. SmartBits increases multicast group count from 8 to 32 by increments of 8. Configure one flow per transmitter (a single transmitter and receiver ONLY). Configure a non-member receive port to monitor stray frames. Configure SmartMulticastIP in step mode with the following settings:

- Initial rate 40%
- Maximum rate 100%
- Step rate 20%
- Initial group count 8
- Step group count 8
- Maximum group count 32

(d) Forwarding Latency. Switches are configured for maximum load using 64, 256, 1408, and 1518-byte packets. Minimum latency, maximum latency, and average latency are recorded for each receiver port in each multicast group at each packet size.

(e) Max Group Capacity. Configure SmartMulticastIP for maximum group capacity. Configure one transmitter port and one receiver port. Configure an initial group count of 50 with a step count of 50 groups to get a rough estimate of the maximum number of multicast groups. Once this number is determined, reconfigure SmartMulticastIP with the following settings to successively join more groups and determine the maximum:

- Rate 10%
- Initial group count 1
- Step group count 1

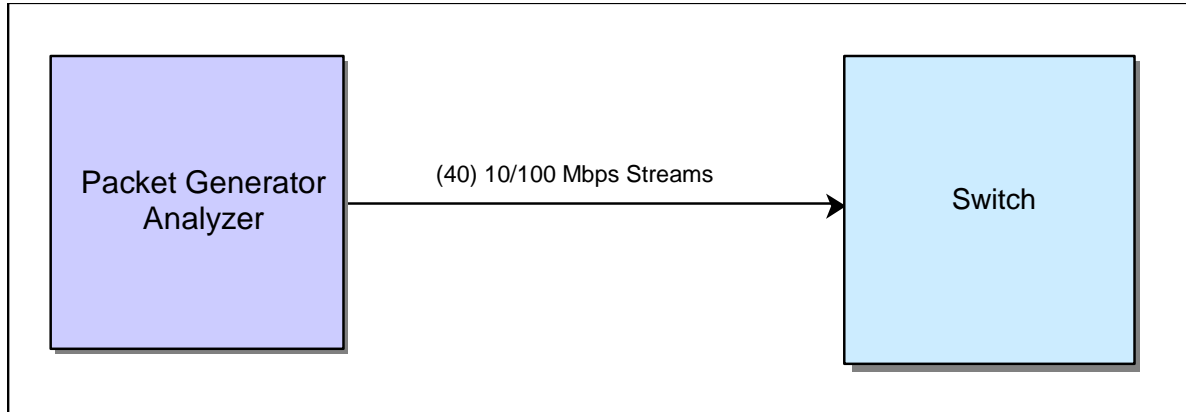
(4) Record results in [Table A-17](#).

(5) FAIL if the device doesn't support multicast or if packets are dropped with 60% multicast load using 16 groups.

### 2.2.10 Core 10/100-Port Performance

a. **Objective.** Test objective is to measure the 10/100-port performance of the core switch using layer 2 and layer 3 traffic.

b. **Configuration.** Figure 19 shows the Core 10/100-Port Performance test configuration. SmartBits is connected to the core switch with forty 100-Mbps streams, twenty to each 10/100 module.



**Figure 19. Core 10/100-Port Performance Configuration**

c. **Procedure.**

(1) Configure the test analyzer to transmit 40 full-duplex 100-Mbps streams to the core switch, 20 to each 10/100 module. Configure the switch for layer 2 traffic.

(2) Use SmartFlow to perform the Throughput and Jumbo tests in a full mesh mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.

(3) Repeat this test using layer 3 traffic.

(4) Record results in [Table A-18](#).

(5) PASS if throughput is 75% or greater for all packet sizes.

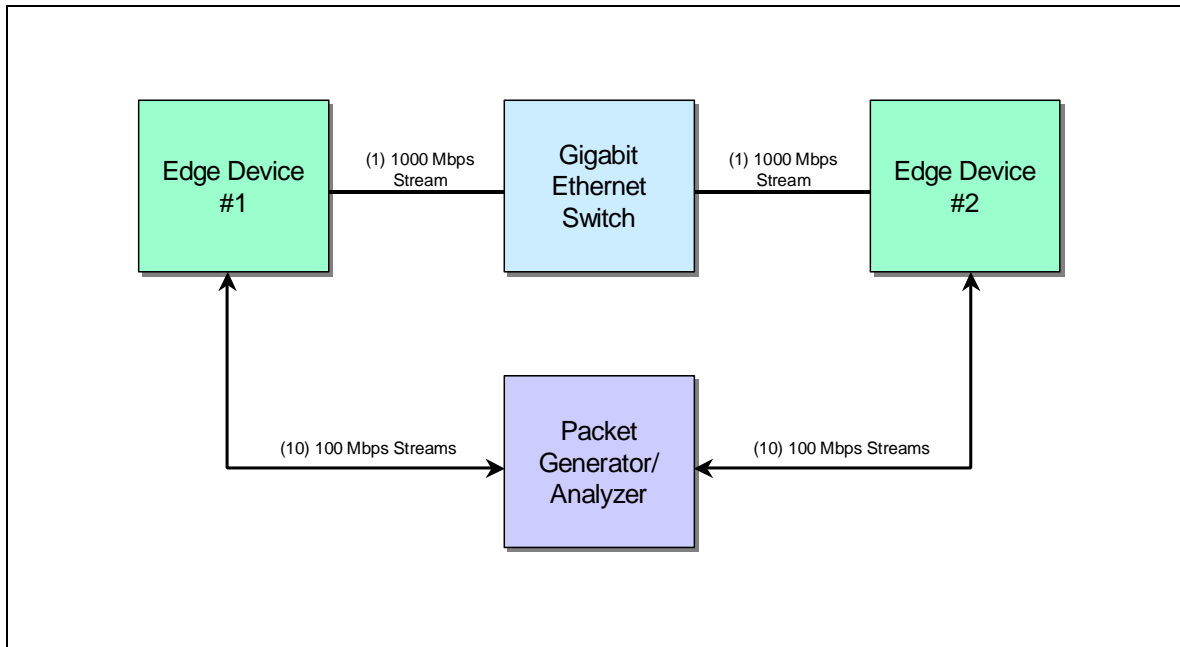
## 2.3 Combined Edge/Core Performance

### 2.3.1 Bridging

a. **Objective.** Test objective is to verify interoperability of edge device and core switch 1000-Mbps interfaces and to measure the performance when bridging layer 2 traffic between 100-Mbps and 1000-Mbps interfaces.

b. **Configuration.** Figure 20 shows the Bridging test configuration. SmartBits is connected to two edge devices with ten 100-Mbps streams to each edge device. Each edge device is connected to the core switch with one 1000-Mbps stream.





**Figure 20. Bridging Configuration**

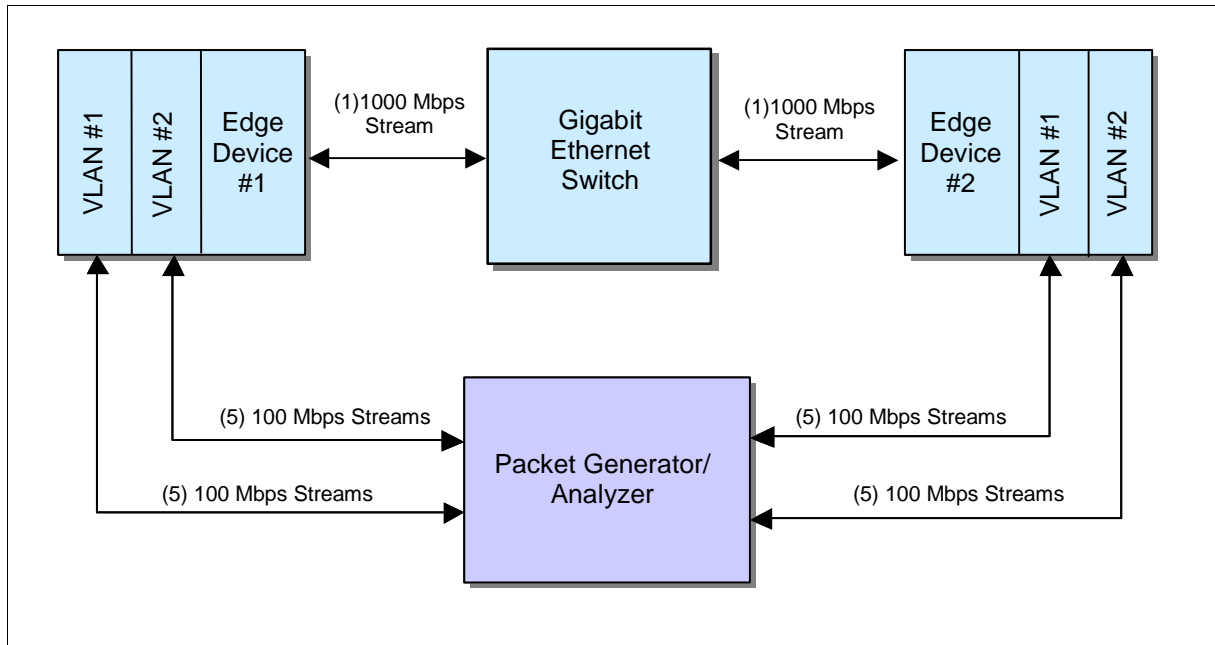
**c. Procedure.**

- (1) Configure SmartBits to transmit 10 full-duplex 100-Mbps streams to each edge device.
- (2) Use SmartFlow to perform the Throughput and Jumbo tests in backbone mode. Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.
- (3) Record results in [Table A-19](#).
- (4) PASS if throughput is 75% or greater for all packet sizes.

**2.3.2 Broadcast Distribution and Leak**

a. **Objective.** Test objective is to verify multiple broadcast streams remain in their designated VLAN.

b. **Configuration.** Figure 21 shows the Broadcast Distribution and Leak test configuration. SmartBits is connected to two edge devices with ten 100-Mbps streams to each edge device. The edge devices are configured for two VLANs with five ports in each VLAN. VLANs on one edge device correspond to the VLANs on the second edge device. Each edge device is also connected to a core switch with one 1000-Mbps stream using 802.1Q VLAN tags.



**Figure 21. Broadcast Distribution and Leak Configuration**

**c. Procedure.**

(1) Configure five 100-Mbps Fast Ethernet ports on each edge device in VLAN 1. Configure five 100-Mbps Fast Ethernet ports on each edge device in VLAN 2

(2) Configure two ports on the core switch in one VLAN. Configure all the other ports in another VLAN. Connect two other 1000-Mbps ports to the core switch to monitor broadcast leakage.

(3) Configure SmartBits for two VLANs. Use SmartWindow to transmit broadcast traffic within VLAN 1. Verify traffic remains in VLAN 1 on both edge devices. Verify no traffic leaks into VLAN 2 on either edge device.

(4) Verify core traffic appears only on the two core switch ports in use.

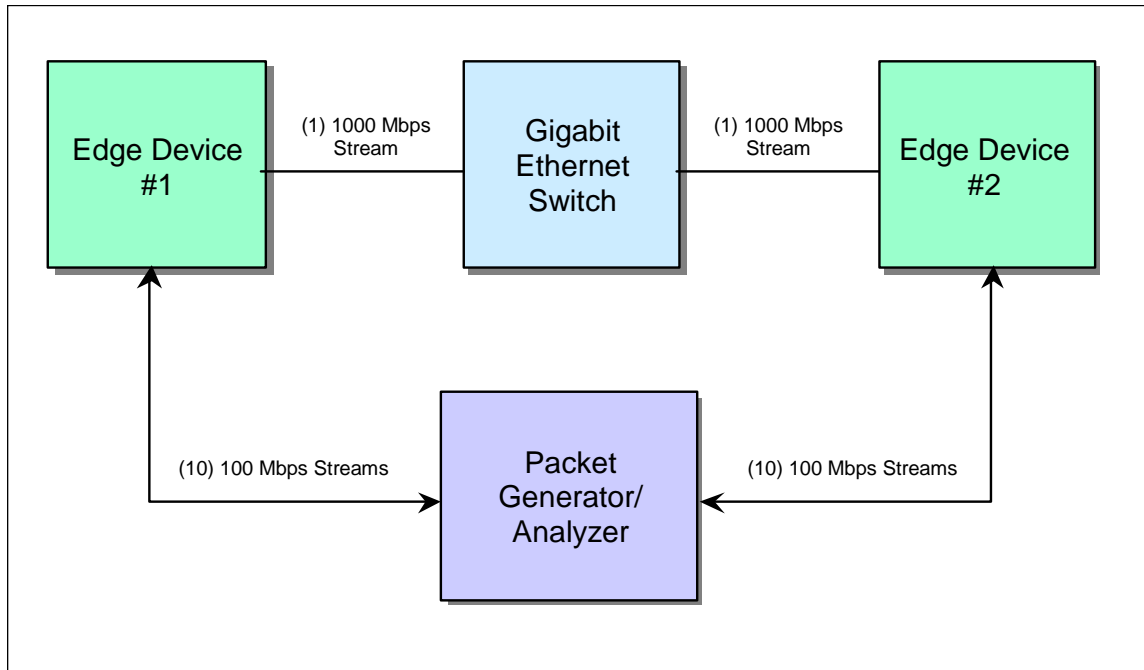
(5) Record results in [Table A-20](#).

(6) FAIL if traffic leaks from one VLAN to another or if traffic is not distributed within its own VLAN.

### 2.3.3 Edge Routing

a. **Objective.** Test objective is to measure throughput while the edge device forwards layer 3 IP traffic between 100-Mbps and 1000-Mbps interfaces and to verify interoperability of the edge and core switch 1000-Mbps interfaces.

b. **Configuration.** Figure 22 shows the Edge Routing test configuration. SmartBits is connected to two edge devices with ten 100-Mbps streams to each edge device. Each edge device is connected to the core switch with one 1000-Mbps stream.



**Figure 22. Edge Routing Configuration**

**c. Procedure.**

(1) Configure the switch for layer 3 switching via OSPF. Configure SmartBits to transmit 20 streams, 10 per edge device, with each 100-Mbps stream as a separate subnet.

(2) Use SmartFlow to perform the Throughput and Jumbo tests in backbone mode. Perform these tests on 128, 256, 512, 1024, 1280, and 1518-byte frame sizes in the following two scenarios:

- (a) Configure layer 3 IP routing only on the core switch.
- (b) Configure layer 3 IP routing on both the edge and the core switch.

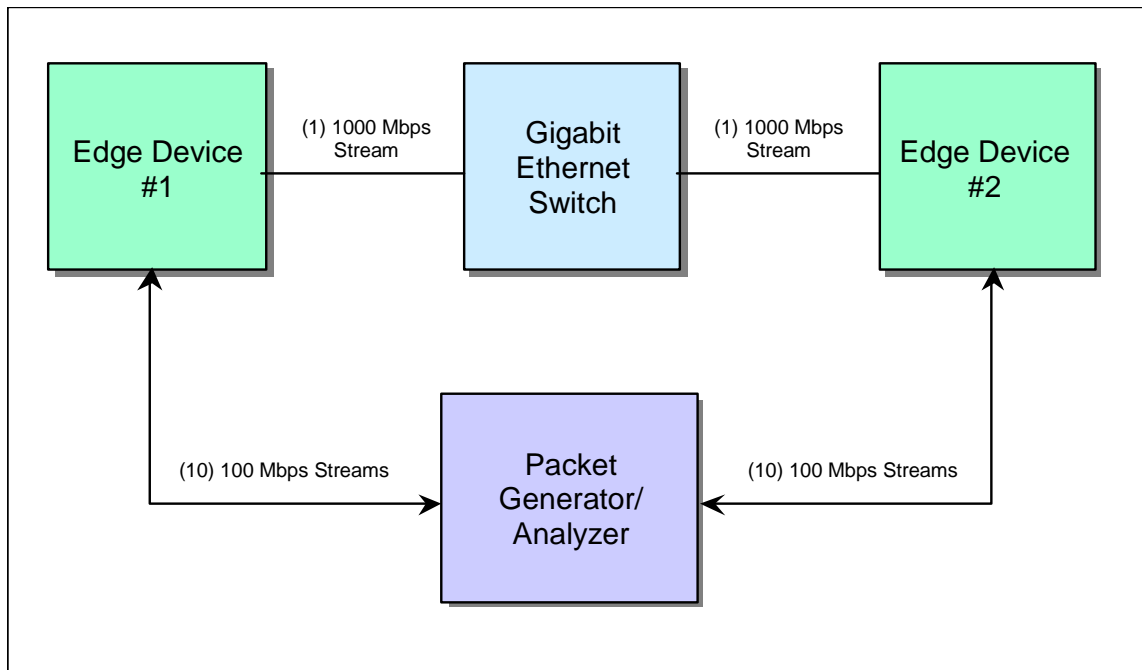
(3) Record results in [Table A-21](#).

(4) FAIL if edge device does not support layer 3 routing or if edge device interferes with core routing.

**2.3.4 VLAN Tagging – Bridging and Routing**

a. **Objective.** Test objective is to verify bridging and routing performance while using 802.1Q VLAN tags.

b. **Configuration.** Figure 23 shows the VLAN Tagging – Bridging and Routing test configuration. SmartBits is connected to two edge devices with ten 100-Mbps streams to each edge device. Each edge device is connected to the core switch with one 1000-Mbps stream. There are three configurations: 1) Bridging 10 VLANs, same 10 VLANs on both edge devices, 2) Routing 20 VLANs, 10 different VLANs on each edge device, and 3) Routing 20 VLANs with ACLs.



**Figure 23. VLAN Tagging – Bridging and Routing Configuration**

**c. Procedure.**

(1) Connect SmartBits to the two edge devices with ten 100-Mbps streams. Connect edge devices through the core switch using single 1000-Mbps connections with 802.1Q VLAN tags. Perform the following three subtests:

(a) Bridging with 10 VLANs. Configure SmartBits to transmit tagged traffic from 10 VLANs on one edge device to the same 10 VLANs on another edge device. Verify traffic is bridged properly. Use SmartFlow to perform the Throughput and Jumbo tests in a port-pair configuration.

(b) Routing with 20 VLANs. On each edge device configure each 100-Mbps port as a separate VLAN with VLAN tags. Use Table G-8 for the IP addressing scheme. Configure SmartBits to transmit IP traffic via 20 VLANs, 10 per edge device, tagging each 100 Mbps stream. Verify the switch correctly routes tagged IP traffic over multiple VLANs. Use SmartFlow to perform the Throughput and Jumbo tests in full mesh mode.

(c) Routing with ACLs. Using the Routing with 20 VLANs configuration, apply an ACL to determine the effect on switch performance. Use SmartFlow to perform the Throughput and Jumbo tests in full mesh mode.

(2) Perform these tests on 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.

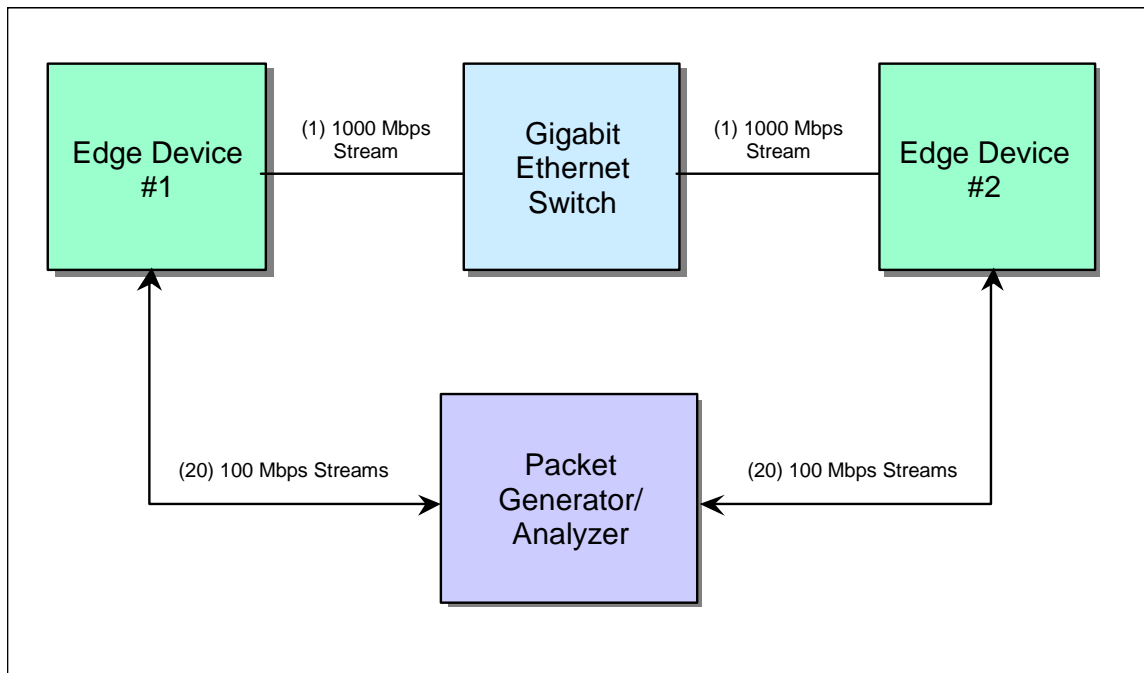
(3) Record results in [Table A-22](#).

(4) FAIL if packets are not properly bridged or routed.

### **2.3.5 Multicast Performance**

a. **Objective.** Test objective is to measure multicast performance on the combined edge/core including the maximum number of multicast groups supported by the devices.

b. **Configuration.** Figure 24 shows the Multicast Performance test configuration. SmartBits is connected to each edge device with twenty 100-Mbps streams. Each edge device is connected to the core switch with a 1000-Mbps link.



**Figure 24. Multicast Performance Configuration**

c. **Procedure.**

(1) Enable IGMP snooping on the edge devices, and OSPF and PIM on the core switch. Use DVMRP if PIM is not supported. Configure SmartBits to transmit 40 streams of multicast traffic for frame sizes 64, 1408, and 1518 to the edge devices.

(2) Use SmartMulticastIP to perform each of the four following subtests:

(a) **Multicast Traffic.** Configure SmartMulticastIP for multicast only traffic. Configure 20 streams belonging to one subnet and 20 streams belonging to a second subnet. Configure 12 multicast groups with 6 transmitters on each edge device. Configure each of the 12 multicast groups with the transmitter on one edge device and one receiver on each edge device. Configure SmartMulticastIP in step mode with the following settings:

- Group count            1
- Initial rate            40%
- Maximum rate        100%
- Step rate              20%

(b) **Multicast and Unicast Traffic.** Configure SmartMulticastIP for multicast and unicast traffic. Use the same 12 groups as the multicast traffic subtest, but gradually introduce unicast traffic at the same rate as the multicast traffic. Configure SmartMulticastIP in step mode with the following settings:

- Group count            1

- Initial rate 10%
- Maximum rate 50%
- Step rate 10%

(c) Scaled Group Forwarding. Configure SmartMulticastIP for Scaled Group forwarding. SmartBits increases multicast group count from 8 to 32 by increments of 8. Configure one flow per transmitter (a single transmitter and receiver ONLY). Configure a non-member receive port to monitor stray frames. Configure SmartMulticastIP in step mode with the following settings:

- Initial rate 40%
- Maximum rate 100%
- Step rate 20%
- Initial group count 8
- Step group count 8
- Maximum group count 32

(d) Forwarding Latency. Switches are configured for maximum load using 64, 1408, and 1518-byte packets. Minimum latency, maximum latency, and average latency are recorded for each receiver port in each multicast group at each packet size.

(e) Max Group Capacity. Configure SmartMulticastIP for Max Group Capacity. Configure one transmitter port and one receiver port. Configure an initial group count of 50 with a step count of 50 groups to get a rough estimate of the maximum number of multicast groups. Once this number is determined, reconfigure SmartMulticastIP with the following settings to successively join more groups and determine the maximum:

- Rate 10%
- Initial group count 1
- Step group count 1

(3) Record results in [Table A-23](#).

(4) FAIL if the device doesn't support multicast or if packets are dropped with 60% multicast load using 16 groups.

### 3.0 SYSTEM FUNCTIONALITY

System level tests are designed to evaluate functionality and reliability of the test network. System functionality does not necessarily reflect the capacity of the DUT but more importantly reflects consistency throughout the duration of the test. Remote terminal emulation systems run preprogrammed scripts to measure selected performance parameters of the network after the test network is configured.

#### 3.1 Overview

System level tests measure the performance of all devices as a complete system. There are 6 edge devices, 4 core switches, and 36 RTE computers installed in a configuration resembling the CUITN architecture to provide user loading that simulates real-world conditions. Each RTE provides two 100-Mbps connections resulting in twelve 100-Mbps

connections to each edge device. Edge devices 1 through 4 are each connected to core switch #1 with one 1000-Mbps link. Edge devices 5 through 8 are each connected to core switch #4 with one 1000-Mbps link each. The four core switches are connected in a partial mesh using 1000-Mbps links. Four tests are conducted using two different configuration scenarios. The four test areas are: File Transfer Protocol (FTP) series, Mix, Multicast, and Fail-over. They are performed for both the 6-subnet and 6-VLAN configurations. When completed, the tester will have a measure of the reliability and functionality of the network when implemented into a live system. The RTE system accumulates statistics on each test it performs. Worldwide web (WWW), FTP, structured query language (SQL), and Simple Mail Transfer Protocol (SMTP) are individually logged accumulatively upon each successful completion of the transaction or session. Timeouts occur at 1 minute if a transaction has not yet been completed. Upon a timeout, the RTE logs the timeout, abandons the transaction, and executes another with no “think delay.” See Appendix B for system functionality data tables.

### 3.2 System Functionality Tests

#### 3.2.1 FTP Series

a. **Objective.** Test objective is to measure forwarding performance for varying loads and traffic patterns of FTP traffic and to measure the device’s ability to load share traffic across equal cost paths via OSPF equal-cost multi-path and with no equal-cost multi-path.

b. **Configuration.** This test is performed on both the 6-subnet and 6-VLAN configurations. Refer to Appendix H for 6-VLAN and 6-subnet configuration details. Figure 25 shows the FTP Series Logical Traffic Flow for 6-subnet.

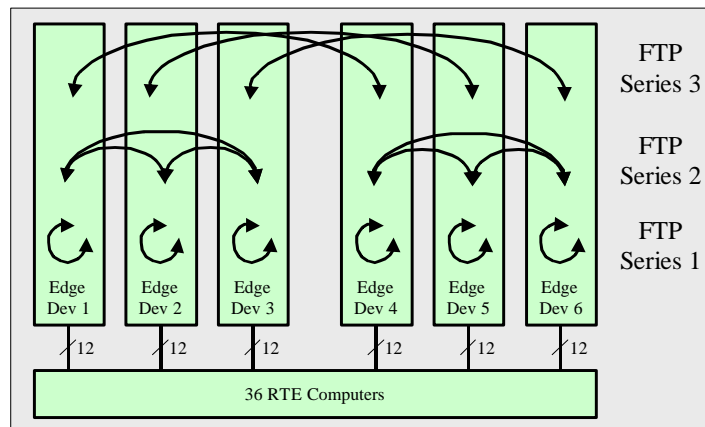


Figure 25. FTP Series Logical Traffic Flow for 6-Subnet

c. **Procedure.**

(1) There are three different series performed in this test. Each series consists of four functionally identical programs starting with 32 users in the first program, then 64 in the second, 128 in the third, and finally 256 users in the fourth. Each program is a 7-minute run of FTP “put” and “get” commands on a 4-megabyte (MB) text file and are executed with no “think delay” between the commands. The RTE users initially perform FTP and login as a “root” user to a designated server before it begins its 7-minute run and transaction logging.

(2) Run FTP Series 1. Traffic originates and terminates within the same edge device. In the 6-subnet, the traffic stays within tier 1.

(3) Run FTP Series 2. Traffic originates from one edge device to another edge device on the same side of the core. In the 8-subnet, the traffic extends to network level 2 but returns to the same side of the core.

(4) Run FTP Series 3. Traffic flows from one edge device to another edge device on opposite sides of the core. This series is performed with OSPF equal-cost multi-path switched off and then again with OSPF equal-cost multi-path switched on.

(5) Because of the 6-VLAN architecture of this network, all three FTP series test traffic flows into or through the core because all traffic is destined to either a different subnet or to a different edge device.

(6) Record results in [Table B-1](#).

(7) FAIL if users do not pass traffic or if throughput rates vary greatly between users.

### 3.2.2 Overnight

a. **Objective.** Test objective is to measure the test network throughput with a mix of various types of unicast and multicast traffic.

b. **Configuration.** This test is performed on both the 6-subnet and 6-VLAN configurations. Refer to Appendix H for 6-VLAN and 6-subnet configuration details.

c. **Procedure.**

(1) Run all four phases of the RTE scripts (Pulse, Soak, Mix, and Multicast Mix) against the 6-subnet and 6-VLAN configurations. The tests for these phases include WWW “pulse,” continuous WWW, FTP, SQL, and e-mail.

(a) WWW Pulse. The network is subjected to 2,520 WWW users pulling real web pages from 36 servers. There are two repetitions of a 15-minute full-speed Hypertext Transfer Protocol (HTTP) transfer and a 45-minute idle time to allow timeouts to age out. The web pages being downloaded contain three HTML pages and nine 200-kilobyte (kB) Graphic Interchange Format (GIF) images.

(b) Soak. The network is subjected to four different traffic types (WWW, FTP, SQL, and e-mail) for 1 hour. Each traffic type workload is configured as 2,520 users in the  $n*(n-2)$  configuration. The following paragraphs describe the four different traffic types.

- WWW Continuous - This is another WWW test identical to the WWW Pulse test but runs continuously for 1 hour with no rest period.
- FTP - This test consists of 1,296 users performing FTP Puts and Gets, alternating between the two. The FTP session is established at the start of the test and the users continuously alternate between an FTP “get” and an FTP “put” command of a 4-MB file. Each command execution is logged upon each successful completion.
- SQL - This test consists of 2,520 users, each performing SQL queries on the default mysql database loaded on the LINUX servers. The queries consist of requests listing table entries and row counts of some of the default tables in the database.



- E-Mail SMTP - The RTE computers use qmail for the SMTP message agent. The test consists of 2,520 users that send and receive varying size mail with SMTP servers.

(c) Unicast Mix. This 2-hour test performs a combination of WWW, FTP, SQL, and SMTP traffic in an  $n*(n-1)*2$  configuration. This creates 2,520 streams with the following traffic ratio: 65% WWW, 20% SMTP, 10% SQL, and 5% FTP.

(d) Multicast/Unicast Mix. This 4-hour test is divided into two sections. The first section performs a combination of unicast traffic consisting of WWW, FTP, and SMTP traffic for the first 2 hours of the test. In the second section multicast traffic is added to the existing unicast traffic. For the remainder of the test, traffic is a combination of multicast and unicast traffic. The test is designed so that 12 designated RTE computers are excluded from any unicast traffic and are instead used to transmit and receive multicast streams at a rate of 5% load on each of the six 100-Mbps links. The unicast mix is run to establish a baseline, and then multicast is added to show any global effects it may have on the unicast traffic. The traffic ratio among the various types of traffic remains constant throughout the test.

(2) Record results in [Table B-2](#).

(3) FAIL if unicast throughput varies by more than 10% from the unicast baseline or if unicast throughput varies by more than 10% from the unicast baseline when multicast traffic is introduced.

### 3.2.3 Network Recovery

a. **Objective.** Test objective is to measure network recovery time during fail-over and recovery when subjected to link and device failures and to verify standby routing functionality.

b. **Configuration.** This test is performed on both the 6-subnet and 6-VLAN configurations. Refer to Appendix H for 6-VLAN and 6-subnet configuration details. Also, refer to Figure 25.

c. **Procedure.**

(1) Use the RTEs to generate FTP and ICMP traffic to provide a visual indicator of network status while this test is in progress. Run FTP series 3, using the 256-user program, to monitor traffic flow and use the ping script, sequencing pings through all the RTE computers to monitor route convergence. Watch network activity bars on the RTE graphical user interface (GUI) for changes in the traffic pattern as links and devices are brought down and restored. Perform the test a second time running a multicast test with six transmitters, three on each side of the core and each having six receivers evenly spread across the edge devices.

(2) Verify the following during fail-over and recovery:

(a) Cutover to redundant IP routing with device or link failure - OSPF equal cost multi-path or redundant routing protocol such as Virtual Router Redundancy Protocol (VRRP).

(b) Edge device redundant gigabit uplink cutover with device or link failure.

(c) Recovery after gigabit switch reboot: Area distribution node 1 (ADN 1) and ADN 2.

(d) Recovery after edge device reboot: edge device #1 and edge device #5.

(e) Fabric redundancy check.

(f) Processor redundancy check.

(g) Power supply redundancy check.

(3) Layer 2 and Layer 3 Edge - Edge device #1 is dual homed to both ADNs as shown in Figures 25 and 26 for the 6-subnet and Figure 27 for the 6-VLAN. Verify the following:

(a) Verify that ADN 1 has control of the gateway then pull the link between ADN 1 and the edge device. ADN 2 should take control of the gateway.

(b) Once ADN 2 has assumed control, restore the link. ADN 1 should regain control if VRRP is used. ADN 2 may retain control if another redundancy method is used.

(c) Once the network has stabilized, pull the link between ADN 2 and the edge device.

(d) Restore the link after verifying that nothing has changed.

(e) Power down ADN 1. ADN 2 should assume control.

(f) Restore power to ADN 1 and wait for the network to stabilize.

(g) Power down ADN 2. Verify nothing happens, unless ADN 2 had control of the gateway.

(h) Once the network has stabilized, restore power to ADN 2.

(4) Layer 3 Core – Power down each ADN and main control node (MCN) to see the effect on the network. Restore each device before the next device is powered down. Pull the inter-core links one at a time to see the effect on the network.

(5) Record results in [Table B-3](#).

(6) FAIL if edge device does not fully recover within 5 minutes or if core does not fully recover within 5 minutes. FAIL if the network cannot re-converge all routing processes and reestablish traffic flows of all types. FAIL if the network cannot recover within 10 seconds when the disrupted system is brought back into normal service.

### 3.2.4 Multicast Streams

a. **Objective.** Test objective is to measure the networks forwarding performance and functionality for varying loads and traffic patterns of IP multicast.

b. **Configuration.** Refer to Appendix H for 6-VLAN and 6-subnet configuration details. See Figure C-6 for a depiction of the logical traffic flow as it is described in this test. The 6-subnet and 6-VLAN architectures are both tested. The network is enabled with Protocol Independent Multicast-Dense Mode (PIM-DM) multicast routing and IGMP version 2 snooping. A network analyzer is placed in line on one of the RTE client's network connections to analyze IGMP join/leave functionality, multicast IGMP snooping, and multicast source quenching while the test is in operation.

c. **Procedure.**

(1) Run the Multicast Generator (MGEN) suite.

(2) The MGEN suite was developed by the Navy and was modeled to provide the same type of reports as the SmartBits Multicast application. The MGEN suite consists of three programs; a multicast generator, a Dynamic Receiver (DREC) and a multicast calculator (MCALC). The RTE scripts are run to configure, control, and synchronize the MGEN programs on each RTE computer. Each stream in all of these tests is independent of one another in that each has a unique IP address as well as a unique port number assigned by the script. The DREC generates a statistical log of each received packet and is post compiled at the end of each MGEN test.

(3) Run the “runmult” script generating *Progressive and High Capacity Streams*.

This is a series of incrementing multicast streams starting with a single sender generating a stream followed by a receiver on every edge device simultaneously joining with the sender. The receivers remain joined for 5 minutes at which time they simultaneously send leave messages and stop the sender. The test is repeated using four streams, eight streams, etc., stepping four at a time for each repetition until 36 streams along with 288 receivers (36 per edge) has been reached. Each stream is set for 497 packets per second at 1408-bytes per packet. With 36 streams in place, the core encounters an accumulated traffic rate of 252 Mbps from the senders. Each group has receivers on all six edge devices generating a combined rate of about 3 gigabits of multicast traffic. A maximum of 1.5 Gbps of bi-directional traffic is placed on any 1-gigabit link. The thirty-six 10/100-Mbps links used by this test transmits 6 Mbps and receives 84 Mbps of multicast traffic.

(4) Record results in [Table B-4](#).

(5) FAIL if multicast cannot join/leave within a reasonable time or cannot provide minimum rate through the core without dropouts while sending 12 MGENs. Dropouts are periods of inactivity lasting longer than 100 milliseconds or inactivity occurring more than one time in any 3-second period.

### 3.2.5 Multicast Channel Surfing

a. **Objective.** Test objective is to verify the system can handle channel surfing, switching one transmit to one receive every minute.

b. **Configuration.** This test is performed on both the 6-subnet and 6-VLAN configurations. Refer to Appendix H for 6-VLAN and 6-subnet configuration details.

c. **Procedure.**

(1) Perform *Couch Potato Channel Surfing* by running the mcsurf script.

(2) Each RTE transmits one multicast stream to the network for a total of 36 constant streams. Each computer also joins a client to the stream of the next computer in sequence. Every 60 seconds all of the receivers rotate to the next computer by performing a leave and a join. This continues until each receiver has “surfed” all the multicast streams. Also, a network analyzer is placed in line on one of the RTE clients network connections to analyze join/leave functionality, multicast IGMP snooping and multicast source quenching while the test is in operation. Each stream is set for 125 packets per second at 1408-bytes per packet.

(3) Record results in [Table B-5](#).

- (4) FAIL if any group or user receives less than 95% of the traffic.

### 3.2.6 Multicast One-to-Many

a. **Objective.** Test objective is to verify that the system can handle a commander's briefing with two transmitters and 70 receivers, and to measure packet loss during joins/leaves in other users.

b. **Configuration.** This test is performed on both the 6-subnet and 6-VLAN configurations. Refer to Appendix H for 6-VLAN and 6-subnet configuration details. This test is only valid after passing MGEN 1 and MGEN 2.

c. **Procedure.**

(1) Perform *All Eyes on the Podium / Commander's Briefing* by running the "mcpodium" script.

(2) The commander's briefing test consists of two multicast streams. Sender 1 is located on edge 1 and sender 2 is located on edge 5. Thirty-five receivers join sender 1. Later, another 35 receivers join sender 2. Once established, 17 receivers leave sender 1 and then 17 receivers leave sender 2. Once completed, the test ends with the remaining receivers sending leave messages. Each stream is set for 497 packets per second at 1408-bytes per packet.

(3) Record results in [Table B-6](#).

(4) FAIL if any receiver drops from the group.

## 4.0 NETWORK MANAGEMENT

Network Management capabilities are evaluated while the switches are installed in the system test configuration. The Evaluation Team will examine the Simple Network Management Protocol (SNMP) capabilities of network devices and the capabilities of device management products for Network Management Stations (NMS) running Solaris and Windows. The Evaluation Team will assess device responses to various valid and invalid SNMP Management Information Base (MIB) requests, as well as the remote configuration and monitoring capabilities of the device management applications. See Appendix C for network management data tables.

### 4.1 Management Questionnaire

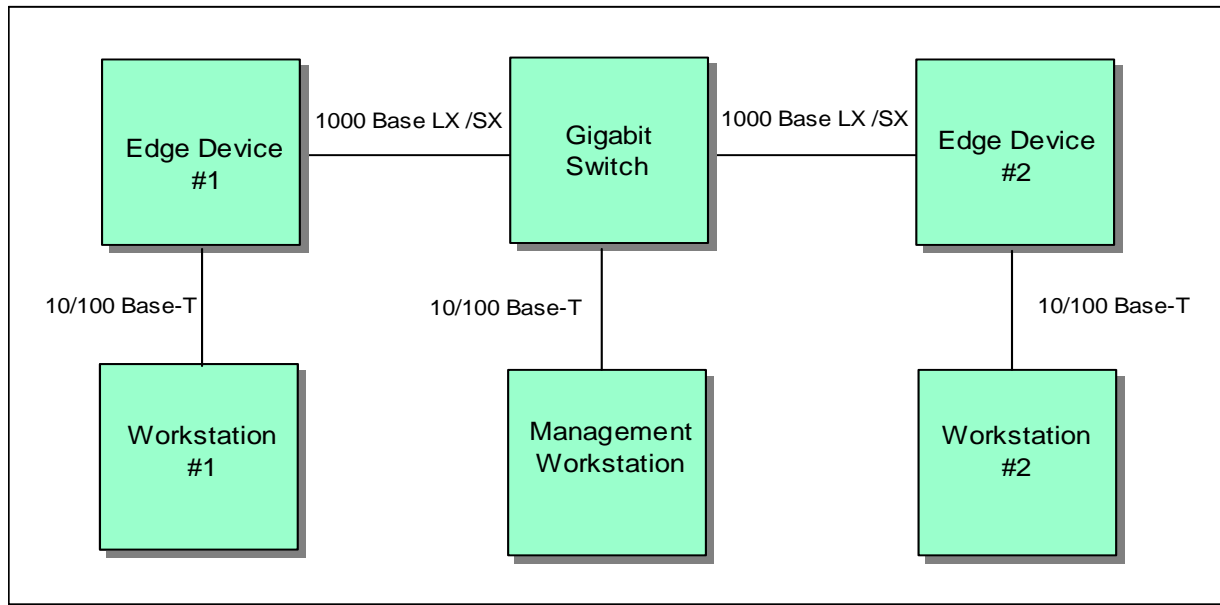
In addition to evaluating NMS capabilities, the Evaluation Team will also gather marketing information from each vendor. This data is collected in a management questionnaire in [Table C-10](#).

### 4.2 Network Management Tests

#### 4.2.1 Telnet – Windows, Solaris, and Linux

a. **Objective.** Test objective is to determine the ability of network devices to accept Telnet connections from systems running various operating systems in a GbE network.

b. **Configuration.** Figure 26 shows the Telnet test configuration (same as NMS configuration). The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.



**Figure 26. NMS Configuration**

**c. Procedure.**

- (1) Contact the network device via Telnet from several platforms, each running a different operating system.
- (2) Verify Telnet connections are established correctly from each platform. The platforms include Solaris, Windows, and Linux.
- (3) Record results in [Table C-1](#).
- (4) PASS if valid Telnet sessions are established from the specified systems.

**4.2.2 SNMP MIB Walk**

a. **Objective.** Test objective is to determine the ability of a network device to provide the standard SNMP MIB (MIB-II) and the vendor's MIB for the requesting Network Management Station (NMS).

b. **Configuration.** Figure 26 shows this test configuration. The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

**c. Procedure.**

(1) Execute SNMP GET and GET-NEXT requests. The network management application requests portions of the MIB tree from the network device, and will display or record the results on the NMS.

(2) The network management application on the NMS starts a "MIB walk" of the MIB-II sub-tree of the SNMP MIB, specifying the IP address and the read-only community string configured on the network device. Inspect the results of the MIB walk to verify all relevant groups of MIB-II returned values. The relevant groups include the system, interfaces, IP, TCP, and SNMP.

(3) Check the interfaces group to verify that all device interfaces are shown, and check the IP group to verify the correct IP address of the network device. A MIB walk of the Remote Monitoring (RMON) MIB will be conducted for the network device. Inspect the results of the RMON MIB walk to verify all relevant groups of RMON are supported. The relevant groups include statistics, history, events, and alarms.

(4) Perform a MIB walk of the vendor MIB, located in the 'private.enterprises.<vendor>' sub-tree for the network device. Inspect the results of the vendor MIB walk to verify that all relevant groups of the vendor MIB returned appropriate values. Repeat the MIB walk and results examinations for other MIBs that the vendor claims to support.

(5) Record results in [Table C-2](#).

(6) FAIL if MIB table information is incorrect, or if requests produce errors.

#### 4.2.3 SNMP SET / GET Requests

a. **Objective.** Test objective is to determine the ability of a network device to respond correctly to SNMP SET and GET requests.

b. **Configuration.** Figure 26 shows this test configuration. The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) The NMS attempts to reset various MIB values on the network device including device port activation, and requests the variable values to verify the change. Verify the state of the network device as matching the MIB variable settings.

(2) The network manager sets the MIB-II system location variable, "system.sysLocation.0," on the selected network device to the string "Bldg. 53302 TIC." Verify the network manager indicates that the set was successful.

(3) The network manager gets the MIB-II system location variable, "system.sysLocation.0," on the selected network device. Verify the network manager indicates that the GET request was successful and that the system location is "Bldg. 53302 TIC."

(4) The network manager verifies that the interface of the network device to which a workstation is attached is up. The network manager turns off the interface of the network device to the attached workstation by setting the interface's variable "interfaces.ifTable.ifEntry.ifAdminStatus.n," where "n" is the interface SNMP index, to "down." Verify that the network manager indicates the set was successful.

(5) The network manager verifies that the interface of the network device to which the workstation is attached is down. The network manager turns the interface of the network device back on by setting the above interface variable to "up" and verifies that the connection to the workstation is re-established.

(6) Record results in [Table C-3](#).

(7) FAIL if information is not correctly stored and recalled, or if ports do not disable and enable correctly.

#### 4.2.4 SNMP Traps

a. **Objective.** Test objective is to determine the ability of network devices to generate SNMP traps for reportable failure conditions and send them to a specified network management station.

b. **Configuration.** Figure 26 shows this test configuration. The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Subject the network device to the following three conditions that should generate SNMP traps. View any received trap events from the network management application on the NMS.

(a) Cycle power on the network device to generate a “cold start” trap.

(b) Reboot the network device by a system reset to generate a “warm start” trap.

(c) Disconnect the cable connecting a workstation to the network device for at least 1 minute to generate a “link down” trap. Reestablishing the connection will generate a “link up” trap. Do not choose the management workstation connection!

(2) Inspect the event log of the management application to verify the four traps were received by the NMS.

(3) Record results in [Table C-4](#).

(4) PASS if traps for link status and at least one type of restart are received for the correct conditions.

#### 4.2.5 SNMP Security

a. **Objective.** Test objective is to determine the ability of a network device to reject SNMP SET and GET requests for unauthorized management stations and incorrect community strings.

b. **Configuration.** Figure 26 shows this test configuration. The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) The NMS attempts to reset various MIB variable values on the network device using the read-only community string and an invalid community string, and requests the variable values when the network device does not have the NMS in its access list. The various requests should time out on the NMS to indicate rejection. Also, an “authentication failure” trap should be sent for each failed request.



(2) Attempt to set the MIB-II system location variable, “system.sysLocation.0,” on the selected network device to the string “TIC LAB,” using the read-only community string of the network device. The network manager times out to indicate that the set failed. “Authentication failure” events are recorded in the network manager application log.

(3) Get the MIB-II system location variable, “system.sysLocation.0,” on the selected network device using the read only community string. The network manager should indicate that the GET request was successful and that the system location is not “TIC LAB.”

(4) Attempt the above operation again, but substitute an invalid community string for the read-only community string for the SET request with the same results as before.

(5) Change the IP address of the NMS in the network device SNMP access list to a different address, using the network device console interface. The address cannot be any “universal access” address. Attempt to get the MIB-II system location variable, “system.sysLocation.0,” on the selected network device using the read-only community string. The network manager should time out to indicate that the GET request failed.

(6) Change the IP address of the NMS in the network device SNMP access list back to the correct address using the network interface device console.

(7) Record results in [Table C-5](#).

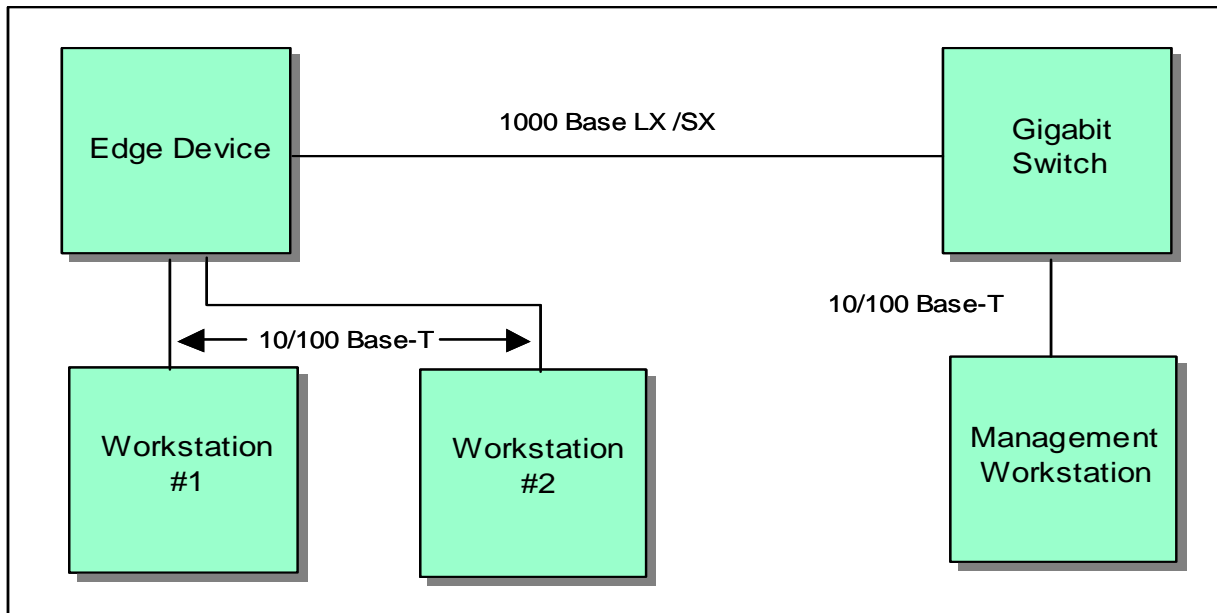
(8) FAIL if device accepts requests from unauthorized stations or accepts SET requests with community strings not granting write permission.

#### **4.2.6 Network Element Configuration**

a. **Objective.** Test objective is to determine the ability to configure a network element from the network management platform using the network element manager or configuration tool.

b. **Configuration.** Figure 27 shows this test configuration. The network will be configured with a switch and an edge device. The management workstation is connected directly to the switch and the two workstations are connected to the edge device via 10/100Base-T Ethernet connections.





**Figure 27. Network Element Configuration**

**c. Procedure.**

(1) Attach the two workstations to the edge device. Use the element manager to configure a subnet and a VLAN. View the configuration of the edge device from the management workstation. Workstation #1 will attempt to communicate with workstation #2.

(2) Inspect the initial configuration of the network element using the element manager to verify that no separate VLAN is configured between workstation #1 and #2. Use the element manager to construct a VLAN named “VLAN\_nm1” between workstation #1 and #2. Verify the element manager displays the new VLAN and that the workstation device ports are members of the VLAN. Workstation #1 will attempt to contact workstation #2 to verify the subnet connection.

(3) Record results in [Table C-6](#).

(4) PASS if VLAN is established and is isolated from other ports.

#### **4.2.7 Port VLAN Identifier**

a. **Objective.** Test objective is to determine whether the network device supports only one Port VLAN Identifier (PVID) per access port.

b. **Configuration.** Figure 26 shows the PVID test configuration (same as NMS configuration). The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

**c. Procedure.**

(1) Assign the PVID to a specific port on the edge device via the management workstation. There should be only one PVID assigned to an access port.

(2) Attempt to assign a second PVID to the same port.

(3) Verify the second attempt fails either by not allowing the reassignment or by changing the PVID to the new one.

(4) Record results in [Table C-7](#).

(5) FAIL if device allows a second PVID assigned to the same port.

#### 4.2.8 Device Performance Monitoring

a. **Objective.** Test objective is to determine the element manager's capability to display port information on the management workstation.

b. **Configuration.** Figure 26 shows the Device Performance Monitoring test configuration (same as NMS configuration). The network will be configured with a switch and two edge devices. The management workstation is connected directly to the switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Attempt to collect port information from a network device to display on the management station console.

(2) Use the element manager to connect to a device within the GbE network, and select a port to be monitored. The port should be one of the ports to which the workstations are connected or a port on the primary path between them. View the collected information on the management station console.

(3) Transfer a file from workstation #1 to workstation #2. This generates traffic on the monitored port.

(4) The element manager should generate a graph or table that shows all traffic and changes on the monitored port. Note the output characteristics including whether the display is tabular or graphical, and whether collected data includes historical trend storage or only current status.

(5) Record results in [Table C-8](#).

(6) PASS if displayed port statistics reflect traffic on the device.

#### 4.2.9 Network VLAN Configuration

a. **Objective.** Test objective is to determine if the element manager can configure a VLAN across the Ethernet network.

b. **Configuration.** Figure 26 shows the Network VLAN test configuration (same as the NMS configuration). The network will be configured with a switch, two edge devices, a management workstation, and two workstations. The management workstation is connected to the core switch. One workstation is connected to edge device #1 via an Ethernet connection. The second workstation is connected to edge device #2 via an Ethernet connection.

c. **Procedure.**

(1) Use the element manager to construct a VLAN named "VLAN\_nm2" between the two workstations on the edge devices. Verify the VLAN connection by contacting workstation #2 from workstation #1.

(2) Use the management workstation to contact one of the workstations in “VLAN\_nm2.” Since there is no layer 3 routing, the attempt should fail verifying proper isolation of “VLAN\_nm2” from the rest of the network.

(3) Record results in [Table C-9](#).

(4) PASS if VLAN is established and is isolated from other ports across the network.

## 5.0 SECURITY

The core switch undergoes a security assessment to determine the security impact when the switch is integrated into the CUITN architecture. Each device is evaluated against a set of security requirements specified in Army Regulation (AR) 380-19 and other Department of Defense (DoD) regulations. The security evaluation procedure in this section is a summary of a larger evaluation procedure. See Appendix D for security data tables D-1 through D-6, which list results for questions asked about each device. Security engineers examine the capabilities of the switch to determine the capability of the component to provide secure management, protect itself from security compromise, and provide security access protection to the connected network assets. Security engineers also use Internet Security Systems (ISS) SafeSuite and Network Associates Incorporated (NAI) CyberCop scanning programs to look for high-risk vulnerabilities in the switches.

It should be noted that this is a limited operational test designed to check against a specific set of security vulnerabilities. The test is not an exhaustive examination and not all of the device’s capabilities or vulnerabilities are examined.

### 5.1 Security Requirement Traceability

The security requirements criteria used in this evaluation are quoted verbatim from the appropriate regulatory documents. The criteria subparagraphs describe the metrics by which the intelligent addressable device is judged to meet or not meet the stated requirements. The following documents are used to evaluate the intelligent addressable device under test:

- a. Information Systems Security [AR 380-19].
- b. Trusted Computer System Evaluation Criteria [DoD 5200.28-Standard (STD)].
- c. Trusted Network Interpretation [National Computer Security Center-Technical Guide (NCSC-TG-005)].
- d. Trusted Network Interpretation Environments Guideline (NCSC-TG-011) (Red Book).
- e. Required network security services have been determined at the TIC via network analysis. They form the basis for the evaluation of the capabilities that network security services offer.

### 5.2 Security Test Methodology

The following techniques will be used to evaluate the intelligent addressable device's compliance with the specified security requirements:

- a. Inspection - Examination of an item or review of design documentation to confirm compliance with specified requirements.
- b. Demonstration - Verification of an operational or functional capability by performance witnessed by a qualified observer. Observance of operation or inspection of generated output data determines compliance with specified requirements.

c. Testing - Performance of functional operations under specified conditions. Testing involves the generation, acquisition, and recording of test data. Compliance with specified requirements is determined by analyzing the data produced by the tests.

d. Analysis - Review or interpretation of analytical or empirical data under defined conditions or reasoning to show theoretical compliance with the specified requirements.

e. Validation – Validation of vendor claims through the Technical Support Office or representative for features and capabilities that cannot be verified by other means.

Figure 28 is a layout of the network configuration that will be used for security testing.

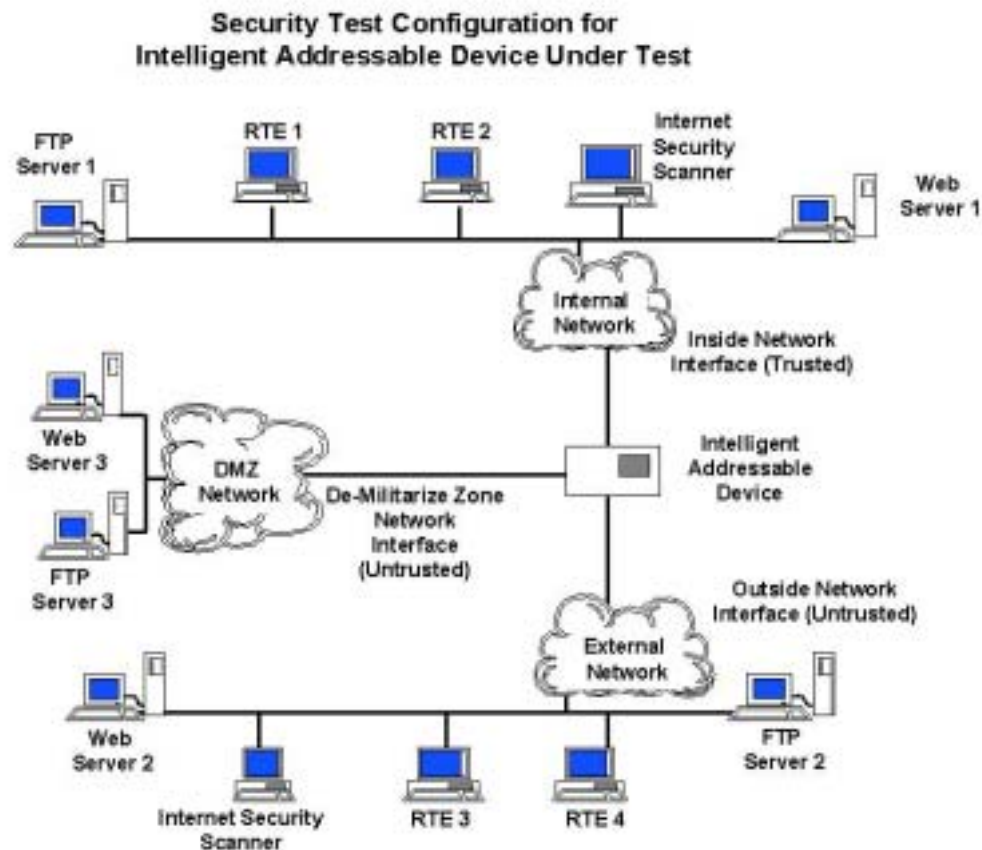


Figure 28. Security Lab Network Configuration

### 5.2.1 Audit Capability

a. **Objective.** Test objective is to verify the switch's ability to export logs to a centralized audit management station, to prevent unauthorized access of the audit trail, to audit security selectable events, to support local or remote network auditing, and to record connection attempts rejected by ACL rules.

b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Enable auditing service. Verify the audit file (syslog) can be exported to another device for storage.

(2) Make changes to the setup configuration. Analyze the audit file and verify product audits all administrative actions.

(3) Scan the product using Cybercop and ISS. Create a VLAN and assign ACL rules. Attempt various types of connections to the product including logins with invalid passwords. Verify all activity is monitored in audit file.

(4) Activate local logging and issue various commands. Log in by remote via Telnet, web, GUI, and SSH to review logs. Activate the syslog service on the management station and issue various commands in the switch management console. Review the audit file locally on the management station. Verify the product allows local and remote auditing.

(5) Setup an ACL and try to connect from an unauthorized IP address. Verify the product records connection attempts rejected by the product's access control rules. Verify the log file shows evidence that the necessary information is recorded in the audit file.

(6) Record results in [Table D-1](#).

(7) FAIL if logs cannot be exported, unauthorized user can change audit trail, audit events are not selectable, or rejected connection events are not recorded.

### 5.2.2 Configuration Management with Secure Remote Management

a. **Objective.** Test objective is to verify the switch's ability to provide full session confidentiality, to secure connections prior to transmission across an untrusted network, to restrict remote administration, to be SNMP/CMIP manageable, and to be remotely managed via web, Telnet and FTP.

b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis, Inspection, and Validation methods are used for this test.

c. **Procedure.**

(1) Using SSH, control the product from a distant location. Log off the remote terminal program and use other options, i.e., Blowfish, DES, and Triple DES. Use a sniffer to view packets from the mirror port. Verify session confidentiality is enforced through negotiation of key exchanges, secure tunneling, signature verification, or encryption algorithms.

(2) Enabled SSH and monitor actions with a sniffer. Verify the product secures the connection prior to transmission across an untrusted network.

(3) Give administrative rights to a specific IP address. Attempt to make changes from another IP address that was not given permissions. Verify the product does not allow remote administration from the second address.

(4) Configure the ACL to log when a device pings the product and log this information on another server. Verify remote managers have the same capability as local managers to view logs, configure filters, and receive alerts.

(5) Configure various password restrictions. Verify the ability to restrict product management to administrators that are collocated with and/or directly connected to the product.

(6) Configure an NT terminal with the management software, Internet Explorer, FTP, and SSH. Initiate management sessions using each of these tools. Verify the product can be remotely managed via web, Telnet, and FTP.

(7) Record results in [Table D-2](#).

(8) FAIL if remote management session is not secure, remote administration is unrestricted, or not remotely manageable via web, Telnet, or FTP. Secure remote management is required on layer 3 switches and preferred, but not required on layer 2 switches.

### 5.2.3 Product Integrity and Assurance

a. **Objective.** Test objective is to verify the switch's ability to set password aging, to protect passwords, to set a password attempt timeout limit, and to require a minimum eight-character password.

b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Verify password aging can be set.

(2) Configure a new password, and then try to read the password file. Verify passwords are protected.

(3) Connect to the switch using Telnet, SSH, and SNMP. Verify the user account is disabled if the user attempts to authenticate more than the established number of authentication attempts.

(4) Review product documentation and set passwords for at least two users. Verify the product can require a minimum eight-character password. Also note if the switch supports the use of the 36 alphabetic-numeric characters.

(5) Record results in [Table D-3](#).

(6) FAIL if password aging, password timeout, or minimum 8-character password cannot be set.

### 5.2.4 Network Based Attack Detection

a. **Objective.** Test objective is to verify the switch's ability to detect and react to network-based attacks, to specify the reaction to the attack, and to provide alerts and instructions to the administrator.

b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Scan the switch using various scanning tools while monitoring the logs. Verify the product has the ability to detect and react to attacks. Include the following:

- Threat profiles (port scans, ping attacks, etc)
- UDP port scans
- TCP port scans
- Ping attacks

- SYN attacks
- IP spoofing attacks
- Ping of death
- ISS attacks

(2) Review product documentation and browse GUI functionality. Verify the switch has the capability to select the events on which to alert or take action and has the ability to execute a predefined, site-configurable “under attack” action. Note whether the switch provides at least one 'under attack' administrator alert.

(3) Verify the switch reacts to the detected attack as established by the system administrator (SA) so that a predetermined action can take place. Predetermined actions may be: trigger an audible alarm, page or send e-mail to the SA, initiate SNMP traps, set up a blind alley, break a network connection, perform special additional auditing, or perform an automatic trace. Verify the switch provides suggested instructions for handling attacks.

(4) Verify the switch reacts to unauthorized login attempts.

(5) Record results in [Table D-4](#).

(6) FAIL if unable to detect attacks or unable to react to attacks.

### 5.2.5 Access Control Filters

a. **Objective.** Test objective is to verify the switch’s ability to associate filters with a specific interface, to perform packet filtering/stateful inspection/proxy, to combine multiple filters on one port, and to change rules without dropping.

b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Configure a filter and associate it with a specific port. Verify the switch is able to associate filters to interfaces/ports (e.g. segment networks, designate administration port, etc).

(2) Set up an ACL and apply it to a port. Attempt to pass traffic through the port that should be filtered out (dropped). Verify the switch can perform packet filtering/stateful inspection/proxy on: IP source address, IP destination addresses, protocol, TCP source port, TCP destination port, source interface, and destination interface.

(3) Attempt to configure multiple ACLs on a single port. Verify the switch allows combining filters to form an aggregate filter of very narrow focus.

(4) Transfer a large file between two machines through the switch. While the transfer is in progress, perform configuration changes. Verify changes can be made without affecting the file transfer.

(5) Record results in [Table D-5](#).

(6) FAIL if unable to associate filters with a specific interface, unable to combine multiple filters on one port, or unable to change rules without dropping traffic.

### 5.2.6 Backup and Redundancy

a. **Objective.** Test objective is to verify the switch’s ability to backup and restore the system configuration.



b. **Configuration.** Figure 28 shows the security lab network configuration. Analysis and Inspection methods are used for this test.

c. **Procedure.**

(1) Save configuration settings and control lists in flash memory. Attempt to copy this file to the administration console machine. Verify system configurations and control lists can be backed up.

(2) Attempt to copy the configuration settings and control lists back to the switch. Verify data can be restored.

(3) Record results in [Table D-6](#).

(4) FAIL if unable to backup and restore system configuration.



**This page is intentionally left blank**



## APPENDIX A. STANDALONE PERFORMANCE DATA

**Table A-1. Single Edge Forwarding Results**

<b>Test Engineer:</b>				<b>Test Date (yymmdd):</b>			
<b>Throughput Scenario</b>	<b>24 Ports 100 Mbps Full Mesh</b>		<b>1 Gbps to 1 Gbps</b>		<b>Ten 100-Mbps Streams to One 1 Gbps</b>		<b>One 1 Gbps to Ten 100-Mbps Streams</b>
<b>Packet Size (Bytes)</b>	<b>%</b>		<b>%</b>		<b>%</b>		<b>%</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Scenario</b>	<b>24 Ports 100 Mbps Full Mesh</b>		<b>1 Gbps to 1 Gbps</b>		<b>Ten 100-Mbps Streams to One 1 Gbps</b>		<b>One 1 Gbps to Ten 100-Mbps Streams</b>
<b>Packet Size (Bytes)</b>	<b>Latency (μs)</b>		<b>Latency (μs)</b>		<b>Latency (μs)</b>		<b>Latency (μs)</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Distribution Scenario</b>	<b>24 Ports 100 Mbps Full Mesh</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>≤ 50000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Distribution Scenario</b>	<b>1 Gbps to 1 Gbps</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>≤ 50000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Comments:</b>							

**Table A-2. Single Edge IFG Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
<b>Interframe Gap Scenario</b>	<b>Forwarding Rate</b>	<b>IFG</b>	<b>Pass or Fail</b>
100 Mbps (Minimum 0.96 $\mu$ s)			
1,000 Mbps (Minimum 0.096 $\mu$ s)			
<b>Comments:</b>			

**Table A-3. Single Edge Congestion Control Results**

Test Engineer:		Test Date (yyymmdd):	
Edge Congestion	100 Mbps		1,000 Mbps
Maximum Forwarding Rate			
Uncongested Port % Loss			
Congested Port % Loss			
Was congestion control supported? (Yes/No)			
Comments:			

**Table A-4. Single Edge Error Filtering Results**

Test Engineer:		Test Date (yyymmdd):
Error Condition	Fast Ethernet Port (P/F)	Gigabit Ethernet Port (P/F)
CRC		
Alignment		
Dribble Bits		
Oversize Packets		
Undersize Packets		
Comments:		

**Table A-5. Single Edge Address Caching Results**

Test Engineer:		Test Date (yymmdd):	
Rate (frames/second)	Fast Ethernet Port	Gigabit Ethernet Port	
10,000			
148,810			
1,488,100			
Comments:			

**Table A-6. Single Edge Port Mirroring Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
<b>Port Mirroring</b>		<b>Fast Ethernet</b>	<b>Gigabit Ethernet</b>
Supported (Y/N)			
Number of Ports			
<b>Comments:</b>			

**Table A-7. Edge Link Aggregation Results**

Test Engineer:		Test Date (yyymmdd):	
Link Aggregation Capability		Gigabit Ethernet	
Pass or Fail			
Load Sharing			
Redundancy			
Comments:			

**Table A-8. Edge 8-Port GbE Throughput Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
<b>Throughput Scenario</b>	<b>8 Ports 1,000 Mbps Full Mesh Forwarding</b>	<b>8 Ports 1,000 Mbps Full Mesh Routing</b>	
<b>Packet Size (Bytes)</b>	<b>%</b>	<b>%</b>	
64			
128			
256			
512			
1024			
1280			
1518			
<b>Latency Scenario</b>	<b>8 Ports 1000 Mbps Full Mesh Forwarding</b>	<b>8 Ports 1000 Mbps Full Mesh Routing</b>	
<b>Packet Size (Bytes)</b>	<b>Latency (μs)</b>	<b>Latency (μs)</b>	
64			
128			
256			
512			
1024			
1280			
1518			

**Table A-8. Edge 8-Port GbE Throughput Results (continued)**

Latency Distribution Scenario	8 Ports 1000 Mbps Full Mesh Forwarding						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1k.	≤ 5k.	≤ 10k.	≤ 50k.
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	8 Ports 1000 Mbps Full Mesh Routing						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1k.	≤ 5k.	≤ 10k.	≤ 50k.
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

**Table A-9. Core 64-Port Performance Results**

Test Engineer:			Test Date (yyymmdd):	
Throughput Scenario	64 Ports 1,000 Mbps Full Mesh Forwarding	64 Ports 1,000 Mbps Full Mesh Routing	64 Ports 1,000 Mbps Pairs Routing w/ACL – Frame Loss*	64 Ports 1,000 Mbps Full Mesh VLAN Tagging
Packet Size (Bytes)	%	%	%	%
64				
128				
256				
512				
1024				
1280				
1518				

Table A-9. Core 64-Port Performance Results (continued)

Latency Scenario	64 Ports 1,000 Mbps Full Mesh Forwarding		64 Ports 1,000 Mbps Full Mesh Routing		64 Ports 1,000 Mbps Pairs Routing w/ACL		64 Ports 1,000 Mbps Full Mesh VLAN Tagging	
Packet Size (Bytes)	Latency (μsec)		Latency (μsec)		Latency (μsec)		Latency (μsec)	
64								
128								
256								
512								
1024								
1280								
1518								
Latency Distributio n Scenario	64 Ports 1,000 Mbps Full Mesh Forwarding							
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	≤ 50000.	
64								
128								
256								
512								
1024								
1280								
1518								
Latency Distributio n Scenario	64 Ports 1,000 Mbps Full Mesh Routing							
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	≤ 50000.	
64								
128								
256								
512								
1024								
1280								
1518								
Latency Distributio n Scenario	64 Ports 1,000 Mbps Routing (Port Pairs) w/ACL							
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	≤ 50000.	
64								
128								
256								
512								
1024								
1280								
1518								

**Table A-9. Core 64-Port Performance Results (continued)**

Latency Distribution Scenario	64 Ports 1,000 Mbps Full Mesh VLAN Tagging						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	≤ 50000.
64							
128							
256							
512							
1024							
1280							
1518							
<b>Comments:</b> * The Access Control List was designed to pass every other UDP port. Throughput at or near 50% is the desired result.							

**Table A-10. Core IFG Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
Interframe Gap Scenario	Forwarding Rate	IFG	Pass or Fail
1,000 Mbps (Minimum 0.096 μs)			
<b>Comments:</b>			

**Table A-11. Core Congestion Control Results**

<b>Test Engineer:</b>		<b>Test Date (yyymmdd):</b>
Maximum Forwarding Rate		
Uncongested Port % Loss		
Congested Port % Loss		
Was congestion control supported? (Y/N)		
<b>Comments:</b>		

**Table A-12. Core Error Filtering Results**

Test Engineer:		Test Date (yyymmdd):
Error Condition	Layer 2 (P/F)	Layer 3 (P/F)
CRC		
Alignment		
Dribble		
Oversize Packets		
Undersize Packets		
Comments:		



**Table A-13. Core Address Caching Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>
<b>Rate (frames/second)</b>	<b>Fast Ethernet Port</b>	<b>Gigabit Ethernet Port</b>
10,000		
148,810		
<b>Comments:</b>		

**Table A-14. Core Port Mirroring Results**

Test Engineer:		Test Date (yymmdd):
Port Mirroring	Gigabit Ethernet	
Supported (Y/N)		
Number of Ports		
Comments:		

**Table A-15. Core Link Aggregation Results**

Test Engineer:		Test Date (yyymmdd):
Link Aggregation Capability	Gigabit Ethernet	
Pass or Fail		
Load Sharing		
Redundancy		
Comments:		

**Table A-16. Core Quality of Service Results**

Test Engineer:				Test Date (yyymmdd):		
VOIP, TELNET, FTP, HTTP				Yes/No		
a. Did the edge device support prioritization and was there packet loss in the lower priority traffic only?						
VLAN						
MAC						
IP Address						
IP Flow						
B. Did the edge device support and honor the priority setting?						
VLAN Prioritization						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Traffic Types	Frame Loss %					
VOIP						
TELNET						
FTP						
HTTP						
Total						

Table A-16. Core Quality of Service Results (continued)

IP Prioritization						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Traffic Types	Frame Loss %					
VOIP						
TELNET						
FTP						
HTTP						
Total						
Traffic Prioritization						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Traffic Types	Frame Loss %					
VOIP						
TELNET						
FTP						
HTTP						
Total						
Application Prioritization						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Traffic Types	Frame Loss %					
VOIP						
TELNET						
FTP						
HTTP						
Total						
802.1P Precedence						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Priority Levels	Frame Loss %					
PRI 0						
PRI 1						
PRI 2						
PRI 3						
PRI 4						
PRI 5						
PRI 6						
PRI 7						
Total						

Table A-16. Core Quality of Service Results (continued)

Latency ( $\mu$ s)						
Load %	50.0000	60.0000	70.0000	80.0000	90.0000	100.0000
Priority Levels	Frame Loss %					
PRI 0						
PRI 1						
PRI 2						
PRI 3						
PRI 4						
PRI 5						
PRI 6						
PRI 7						
Total						
Latency Distribution 100%						
Bucket	$\leq 10.$	$\leq 100.$	$\leq 500.$	$\leq 1000.$	$\leq 5000.$	$\leq 10000.$
Priority Levels	Frame Loss %					
PRI 0						
PRI 1						
PRI 2						
PRI 3						
PRI 4						
PRI 5						
PRI 6						
PRI 7						
Total						
Comments:						

Table A-17. Core Multicast Performance Results

Test Engineer:				Test Date (yyymmdd):		
Mixed Class Throughput Multicast Only	Packet Size (Bytes)	Multicast Loss %	Mixed Class Throughput With Unicast	Packet Size (Bytes)	Multicast and Unicast	
					Multicast Loss %	Unicast Loss %
16 Groups @ 40% Load	64		16 Groups @ 20% Load	64		
	1408			1408		
	1518			1518		
16 Groups @ 60% Load	64		16 Groups @ 30% Load	64		
	1408			1408		
	1518			1518		
16 Groups @ 80% Load	64		16 Groups @ 40% Load	64		
	1408			1408		
	1518			1518		
16 Groups @ 100% Load	64		16 Groups @ 50% Load	64		
	1408			1408		
	1518			1518		
Scaled Group Forwarding	Packet Size (Bytes)	Loss %	Scaled Group Forwarding	Packet Size (Bytes)	Loss %	
8 Groups @ 40% Load	64		16 Groups @ 40% Load	64		
	1408			1408		
	1518			1518		
8 Groups @ 60% Load	64		16 Groups @ 60% Load	64		
	1408			1408		
	1518			1518		
8 Groups @ 80% Load	64		16 Groups @ 80% Load	64		
	1408			1408		
	1518			1518		
8 Groups @ 100% Load	64		16 Groups @ 100% Load	64		
	1408			1408		
	1518			1518		
24 Groups @ 40% Load	64		32 Groups @ 40% Load	64		
	1408			1408		
	1518			1518		
24 Groups @ 60% Load	64		32 Groups @ 60% Load	64		
	1408			1408		
	1518			1518		

Table A-17. Core Multicast Performance Results (continued)

Scaled Group Forwarding	Packet Size (Bytes)	Loss %	Scaled Group Forwarding	Packet Size (Bytes)	Loss %
24 Groups @ 80% Load	64		32 Groups @ 80% Load	64	
	1408			1408	
	1518			1518	
24 Groups @ 100% Load	64		32 Groups @ 100% Load	64	
	1408			1408	
	1518			1518	
	1408			1408	
	1518			1518	
Forwarding Latency Multicast Only	Packet Size (Bytes)	Minimum (μs)	Average (μs)	Maximum (μs)	
1 Group, 100 % Load	64				
	1408				
	1518				
Maximum Group Capacity	Packet Size (Bytes)	Groups		Frame Loss	
10 % Load	64				
Comments:					

Table A-18. Core 10/100 Port Performance Results

Test Engineer:		Test Date (yyymmdd):
Throughput Scenario	40 Ports 100 Mbps Full Mesh Forwarding	40 Ports 10/100 Mbps Full Mesh Routing
Packet Size (Bytes)	%	%
64		
128		
256		
512		
1024		
1280		
1518		

Table A-18. Core 10/100 Port Performance Results (continued)

Latency Scenario	40 Ports 10/100 Mbps Full Mesh Forwarding				40 Ports 10/100 Mbps Full Mesh Routing		
Packet Size (Bytes)	Latency (μs)				Latency (μs)		
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	40 Ports 10/100 Mbps Full Mesh Forwarding						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1k.	≤ 5k.	≤ 10k.	≤ 50k.
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	40 Ports 10/100 Mbps Full Mesh Routing						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1k.	≤ 5k.	≤ 10k.	≤ 50k.
64							
128							
256							
512							
1024							
1280							
1518							
Comments:							

Table A-19. Combined Edge/Core Bridging Results

<b>Test Engineer:</b>		<b>Test Date (yyymmdd):</b>					
<b>Throughput Scenario</b>	<b>Bridging</b>						
<b>Packet Size (Bytes)</b>	<b>%</b>						
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Scenario</b>							
<b>Packet Size (Bytes)</b>	<b>Min Latency (μs)</b>		<b>Avg Latency (μs)</b>		<b>Max Latency (μs)</b>		
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Distribution Scenario</b>	<b>Bridging</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 1000.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Comments:</b>							

**Table A-20. Broadcast Distribution and Leak Results**

<b>Test Engineer:</b>		<b>Test Date (yyymmdd):</b>
<b>Broadcast Handling Capability</b>	<b>Pass / Fail</b>	
Broadcast Distribution		
Broadcast Leak		
<b>Comments:</b>		

**Table A-21. Edge Routing Results**

<b>Test Engineer:</b>		<b>Test Date (yyymmdd):</b>
<b>Throughput Scenario</b>	<b>Routing at the Core 100 Mbps Full Mesh</b>	<b>Routing at the Edge and Core 100 Mbps Full Mesh</b>
<b>Packet Size (Bytes)</b>	<b>%</b>	<b>%</b>
64		
128		
256		
512		
1024		
1280		
1518		
<b>Latency Scenario</b>	<b>Routing at the Core 100 Mbps Full Mesh</b>	<b>Routing at the Edge and Core 100 Mbps Full Mesh</b>
<b>Packet Size (Bytes)</b>	<b>Latency (μs)</b>	<b>Latency (μs)</b>
64		
128		
256		
512		
1024		
1280		
1518		



Table A-21. Edge Routing Results (continued)

Latency Distribution Scenario	Routing at the Core 100 Mbps Full Mesh						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	> 50000.
64							
128							
256							
512							
1024							
1280							
1518							
Latency Distribution Scenario	Routing at the Edge and Core 100 Mbps Full Mesh						
Packet Size (Bytes)	≤ 10.	≤ 100.	≤ 500.	≤ 1000.	≤ 5000.	≤ 10000.	> 50000.
64							
128							
256							
512							
1024							
1280							
1518							
<b>Comments:</b>							

Table A-22. VLAN Tagging - Bridging and Routing Results

Test Engineer:			Test Date (yyymmdd):
Throughput Scenario	Bridging 100 Mbps Port Pairs	Routing 100 Mbps Full Mesh	Routing with ACLs 100 Mbps Full Mesh
Packet Size (Bytes)	%	%	%
64			
128			
256			
512			
1024			
1280			
1518			

Table A-22. VLAN Tagging - Bridging and Routing Results (continued)

<b>Latency Scenario</b>	<b>Bridging 100 Mbps Port Pairs</b>			<b>Routing 100 Mbps Full Mesh</b>		<b>Routing with ACLs 100 Mbps Full Mesh</b>	
<b>Packet Size (Bytes)</b>	<b>Latency (μs)</b>			<b>Latency (μs)</b>		<b>Latency (μs)</b>	
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Distribution Scenario</b>	<b>Bridging 100 Mbps Port Pairs</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 1000.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Latency Distribution Scenario</b>	<b>Routing 100 Mbps Full Mesh</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 1000.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							

**Table A-22. VLAN Tagging - Bridging and Routing Results (continued)**

<b>Latency Distribution Scenario</b>	<b>Routing with ACLs 100 Mbps Full Mesh</b>						
<b>Packet Size (Bytes)</b>	<b>≤ 10.</b>	<b>≤ 100.</b>	<b>≤ 500.</b>	<b>≤ 1000.</b>	<b>≤ 5000.</b>	<b>≤ 10000.</b>	<b>&gt; 50000.</b>
64							
128							
256							
512							
1024							
1280							
1518							
<b>Comments:</b>							

**Table A-23. Combined Edge/Core Multicast Performance**

<b>Test Engineer:</b>				<b>Test Date (yyymmdd):</b>		
<b>Mixed Class Throughput Multicast Only</b>	<b>Packet Size (Bytes)</b>	<b>Multicast Loss %</b>	<b>Mixed Class Throughput With Unicast</b>	<b>Packet Size (Bytes)</b>	<b>Multicast and Unicast</b>	
					<b>Multicast Loss %</b>	<b>Unicast Loss %</b>
12 Groups @ 40% Load	64		12 Groups @ 20% Load	64		
	1408			1408		
	1518			1518		
12 Groups @ 60% Load	64		12 Groups @ 30% Load	64		
	1408			1408		
	1518			1518		
12 Groups @ 80% Load	64		12 Groups @ 40% Load	64		
	1408			1408		
	1518			1518		
12 Groups @ 100% Load	64		12 Groups @ 50% Load	64		
	1408			1408		
	1518			1518		

**Table A-23. Combined Edge/Core Multicast Performance (continued)**

Scaled Group Forwarding	Packet Size (Bytes)	Loss %	Scaled Group Forwarding	Packet Size (Bytes)	Loss %
8 Groups @ 40% Load	64		16 Groups @ 40% Load	64	
	1408			1408	
	1518			1518	
8 Groups @ 60% Load	64		16 Groups @ 60% Load	64	
	1408			1408	
	1518			1518	
8 Groups @ 80% Load	64		16 Groups @ 80% Load	64	
	1408			1408	
	1518			1518	
8 Groups @ 100% Load	64		16 Groups @ 100% Load	64	
	1408			1408	
	1518			1518	
24 Groups @ 40% Load	64		32 Groups, 40% Load	64	
	1408			1408	
	1518			1518	
24 Groups @ 60% Load	64		32 Groups @ 60% Load	64	
	1408			1408	
	1518			1518	
24 Groups @ 80% Load	64		32 Groups @ 80% Load	64	
	1408			1408	
	1518			1518	
24 Groups @ 100% Load	64		32 Groups @ 100% Load	64	
	1408			1408	
	1518			1518	
Forwarding Latency Multicast Only	Packet Size (Bytes)	Minimum (μs)	Average (μs)	Maximum (μs)	
1 Group, 100 % Load	64				
	1408				
	1518				
Maximum Group Capacity	Packet Size (Bytes)	Groups	Frame Loss		
10 % Load	64				
<b>Comments:</b>					

**APPENDIX B. SYSTEM FUNCTIONALITY DATA****Table B-1. FTP Series Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
<b>Tests</b>	<b>Bandwidth (Mbps)</b>		
	<b>6-VLAN</b>	<b>36-Subnet L3 Edge</b>	<b>6-Subnet</b>
<b>FTP Series 1 - Network Tier 1</b>			
54 Simulated Users			
108 Simulated Users			
216 Simulated Users			
432 Simulated Users			
864 Simulated Users			
<b>FTP Series 2 - Network Tier 2</b>			
54 Simulated Users			
108 Simulated Users			
216 Simulated Users			
432 Simulated Users			
864 Simulated Users			
<b>FTP Series 3 - Network Tier 3 with OSPF Multipath</b>			
54 Simulated Users			
108 Simulated Users			
216 Simulated Users			
432 Simulated Users			
864 Simulated Users			
<b>FTP Series 3 – Network Tier 3 without OSPF Multipath</b>			
54 Simulated Users			
108 Simulated Users			
216 Simulated Users			
432 Simulated Users			
864 Simulated Users			
<b>Comments:</b>			

Table B-2. Overnight Results

Test Engineer:				Test Date (yymmdd):		
Tests	6-VLAN		36-Subnet L3 at Edge		6-Subnet	
	Trans- actions	Time- outs	Trans- actions	Time- outs	Trans- actions	Time- outs
<b>Single Type Traffic</b>						
HTTP Pulse						
WWW One-hour Soak						
FTP Get/Put One-hour Soak						
E-MAIL One-hour Soak						
SQL						
Mpeg-1 Video Stream Soak						
<b>Mix Type Traffic</b>						
WWW Mix						
FTP Mix						
Email Mix						
Multicast Mix						
<b>Comments:</b>						

Table B-3. Network Recovery Results

Test Engineer:				Test Date (yymmdd):		
Network Recovery			6-VLAN	36-Subnet L3 at Edge	6-Subnet	
L3 Redundancy	Device Failure	Unicast				
		Multicast				
	Link Failure	Unicast				
		Multicast				
Edge Device Uplink Redundancy	Device Failure	Unicast				
		Multicast				
	Link Failure	Unicast				
		Multicast				
Recovery after Gigabit Switch Reboot	ADN 1	Unicast				
		Multicast				
	ADN 2	Unicast				
		Multicast				

**Table B-3. Network Recovery Results (continued)**

Recovery after Gigabit Edge Device Reboot	Edge Device 1	Unicast			
		Multicast			
	Edge Device 2	Unicast			
		Multicast			
Fabric Redundancy Check		Unicast			
		Multicast			
Processor Redundancy Check		Unicast			
		Multicast			
Power Supply Redundancy Check		Core			
		Edge			
Comments:					

**Table B-4. Progressive Multicast Results**

Test Engineer:			Test Date (yyymmdd):	
Progressive Multicast		Percentage of Traffic Lost		
Senders (Multicast Streams)	Receivers (6 per sender)	6-VLAN	36-Subnet L3 at Edge	6-Subnet
1	6			
6	36			
12	72			
18	126			
24	144			
30	180			
36	216			
Comments:				

**Table B-5. Multicast Channel Surfing Results**

<b>Test Engineer:</b>		<b>Test Date (yymmdd):</b>	
<b>Channel Surf + Channel Stability</b>	<b>6-VLAN</b>	<b>36-Subnet L3 at Edge</b>	<b>6-Subnet</b>
Average Packets Receives			
<b>Comments:</b>			

**Table B-6. Multicast One-to-Many Results**

Test Engineer:		Test Date (yyymmdd):	
Commander's Briefing			
	6-VLAN	36-Subnet L3 at Edge	6-Subnet
Traffic Consistency			
Comments:			

**Table B-7. General Notes on System Testing**

Test Engineer:		Test Date (yyymmdd):	
Vendor	Hardware	Software	
Comments:			
Legend:	NA – Not Applicable to the test configuration NT – Not Tested due to lack of time NF – Not tested because this test is directly dependent on the results of another test that failed functionality or reliance. TD – Technical difficulty in the test platform		



## APPENDIX C. NETWORK MANAGEMENT DATA

**Table C-1. Telnet Results**

<b>Test Engineer:</b>	<b>Test Date</b> <i>(yyymmdd)</i> :	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Telnet Session from Solaris Platform		
Telnet Session from Windows Platform		
Telnet Session from Linux Platform		
<b>Comments:</b>		

**Table C-2. SNMP MIB Walk Results**

<b>Test Engineer:</b>	<b>Test Date</b> <i>(yyymmdd)</i> :	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
MIB-II		
RMON (RFC 1757)		
Vendor MIB		
<b>Comments:</b>		

**Table C-3. SNMP SET/GET Requests Results**

<b>Test Engineer:</b>	<b>Test Date</b> <i>(yyymmdd)</i> :	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Location SET Request		
Location GET Request		
SNMP Index, to “down”		
SNMP Index, to “up”		
<b>Comments:</b>		

**Table C-4. SNMP Traps Results**

<b>Test Engineer:</b>	<b>Test Date</b> <i>(yyymmdd)</i> :	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Cold Start		
Warm Start		
Link Down		
Link Up		
<b>Comments:</b>		

**Table C-5. SNMP Security Results**

<b>Test Engineer:</b>	<b>Test Date</b> ( <i>yymmdd</i> ):	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Read-only Community Failure		
1 <sup>st</sup> GET Request		
Invalid Community Authentication Failure		
2 <sup>nd</sup> GET Request		
3 <sup>rd</sup> (Access List Change) GET Request		
<b>Comments:</b>		

**Table C-6. Network Element Configuration Results**

<b>Test Engineer:</b>	<b>Test Date</b> ( <i>yymmdd</i> ):	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Network Element Monitoring		
<b>Comments:</b>		

**Table C-7. Port VLAN Identifier Results**

<b>Test Engineer:</b>	<b>Test Date</b> ( <i>yymmdd</i> ):	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Port VLAN Identifier		
<b>Comments:</b>		

**Table C-8. Device Performance Monitoring Results**

<b>Test Engineer:</b>	<b>Test Date</b> ( <i>yymmdd</i> ):	
<b>SNMP Management</b>	<b>Pass/Fail</b>	
<b>Device Under Test</b>	<b>Core Switch</b>	<b>Edge Device</b>
Device Name		
Device Performance Monitoring		
<b>Comments:</b>		

**Table C-9. Network VLAN Configuration Results**

<b>Test Engineer:</b>	<b>Test Date</b> (yyymmdd):
<b>Element Manager</b>	<b>Pass/Fail</b>
<b>System Under Test</b>	
System Name	
VLAN Configuration	
VLAN Isolation	
<b>Comments:</b>	

**Table C-10. Management Questionnaire**

<b>Test Engineer:</b>		<b>Test Date</b> (yyddmm):	
<b>DUT Vendor/Product:</b>			
<b>Management Feature/Capability</b>	<b>Result Finding</b>	<b>Not Assessed</b>	<b>Remarks</b>
<b>Management Platform Requirements</b>			
<b>What (Operating System) Platforms are Supported?</b> (Specify versions and levels, as applicable)			
Windows 95/98			
Windows NT			
Windows 2000			
Solaris			
HP-UX			
AIX			
Linux			
<b>System Requirements and Application Compatibilities</b>			
Processor/CPU Type and Speed			
RAM Type and Size			
Hard Disk Size			
Swap Space			
Monitor Resolution			
NIC Speeds Supported			
Miscellaneous Hardware (CD-ROM, tape, audio, etc.)			
Operating System (include patch level)			
Additional Utility/Language Supported (X, Java, PERL, Option Pack, etc.)			
Enterprise-level Network Management System			
Web Browser			
Database Systems			

**Table C-10. Management Questionnaire (continued)**

Does Element Manager limit access to specified users, or provide other security features to limit use?			
<b>Network Element SNMP Agent Capabilities</b>			
What versions of SNMP does the network element agent support (e.g., v1, v2, v3)?			
Are SNMP "set" commands supported by the agent?			
Can SNMP "set" commands be disabled or otherwise limited (e.g., access lists)?			
Does the basic device support RMON (with no additional/unbundled hardware or software)?			
<b>Which RMON Groups are Supported?</b> (*Indicates the four basic RMON groups typically implemented)			
Statistics Group*			
History Group*			
Alarm Group*			
Event Group*			
Hosts Group			
HostTop N Group			
Matrix Group			
Filter Group			
Packet Capture Group			
Are MIBs other than basic SNMP MIB II (RFC 1213) and RMON (RFC 1757) supported?			
<b>What Other Standard MIBs are Supported?</b>			
Host Resources MIB (RFC 1514)			
Bridge MIB (RFC 1493)			
Repeater MIB (RFC 2108, RFC 1516)			
Ethernet-like Interfaces MIB (RFC 1643)			
OSPF MIB (RFC 1850)			
RMON2 MIB (RFC 2021)			
Others (specify)			
<b>What Standard SNMP Traps Below are Supported?</b>			
Cold Start			
Warm Start			
Link Up			
Link Down			
Authentication Failure			

**Table C-10. Management Questionnaire (continued)**

<b>Network Element SNMP Agent Security</b>			
Are SNMP management station access lists, or other management station authentication methods, supported?			
How many managers can be specified/allowed in access lists?			
How many SNMP trap receivers can be specified on a device agent?			
<b>Web-based Management and Security</b>			
Do network elements have web browser management support?			
What web browsers are compatible with network elements for management?			
Are features such as Java applet support required for web browser use? Required features include: Java, ActiveX, other (specify).			
What security methods are used for web-based management?			

**This page is intentionally left blank.**

## APPENDIX D. SECURITY DATA

**Table D-1. Audit Results**

Reference	Operational Requirements	Y / N?
Audit NCSC-TG-005 (2.2.2.2)	Does the product export audit logs to a centralized audit management station for analysis?	
	Is the product capable of auditing all administrative actions?	
	Does the product's audit mechanism selectively audit any security related product event?	
	Does the product allow local or remote network auditing by the SA?	
	Does the product record connection attempts rejected by the product's access control rules (an unauthorized IP address trying to connect)?	
	Does the product: <ul style="list-style-type: none"> <li>• Create audit trail data</li> <li>• Maintain audit trail data</li> <li>• Protect audit trail data from modification</li> <li>• Protect audit trail data from unauthorized access</li> <li>• Protect audit trail data from destruction</li> </ul>	
	Does the product's audit mechanism format reports in useful, human readable form?	
	Does the product log date, time, source address, destination address, and session oriented event (e.g., FTP get, FTP put, FTP cd, HTTP, Telnet UID, and Password)?	

**Table D-2. Configuration Management with Secure Remote Management Results**

Reference	Operational Requirements	Y / N?
Other Security Services NCSC-TG-005 (9.3.1)	Does the product demonstrate full session confidentiality (e.g., through negotiation of key exchange, secure tunneling, signature verification or encryption algorithms)?	
	Does the product demonstrate full session integrity enforced through key exchange, secure tunneling, signature verification, and/or encryption algorithms?	
	Can the SA select the security measures to ensure protection of the management link (e.g., key exchange, tunneling, signature verification, and encryption)?	
	Does the product secure the connection prior to transmission across an untrusted network (internal or external)?	

**Table D-2. Configuration Management with Secure Remote Management Results  
(continued)**

	Does the product allow remote administration only from selected IP addresses?	
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Do remote managers have the ability to view logs and reports, configure filters, and receive alerts the same as local managers?	
	Does the product provide the option to be managed by Simple Network Management Protocol/Common Management Informational Protocol (SNMP/CMIP)?	
	Is the product configurable to restrict product management to administrators that are co-located with and/or directly connected to the product?	
System Integrity NCSC-TG-005 (2.2.3.1.2)	Does the product provide hardware and/or software features that can periodically validate the correct operation of the on-site hardware and firmware elements of the product?	
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	What are the ways to manage the device remotely (e.g. web-based, Telnet, FTP)?	

**Table D-3. Product Integrity and Assurance Results**

Reference	Operational Requirements	Y / N?
(AR 380-19, 2-15i)	Does the product set password aging and is it configurable?	
I&A NCSC-TG-005 (2.2.2.1).	Does the product protect the passwords of the product using a mechanism that meets C2 requirements for data protection (e.g., shadow passwords or passwords stored in an encrypted format)?	
	Will the management device limit the number of log-on attempts and set a timeout limit on a password attempt?	
AR 380 – 19 paragraph 2-14i	Can the password length be restricted to a minimum of eight characters <u>and</u> does it support the use of the 36 alphabetic-numeric characters?	



**Table D-4. Network Based Attack Detection Results**

Reference	Operational Requirements	Y / N?
NCSC-TG-005	<p>Is the product capable of detecting:</p> <ul style="list-style-type: none"> <li>• Threat profiles (i.e. port scans, ping attacks, etc.)</li> <li>• UDP port scans</li> <li>• TCP port scans</li> <li>• Ping attacks</li> <li>• SYN attacks</li> <li>• IP spoofing attacks</li> <li>• Ping of death</li> <li>• SATAN attacks</li> <li>• ISS attacks</li> </ul>	
	Does the product have the ability to react to detected intrusions?	
	Is the reaction to detected intrusions predefined, site configurable, and/or selectable?	
	Can the administrator add or configure predefined intrusion events on which to alert?	
	Does the product have the capability to select the events on which to alert or take action?	
	Does the product react to the detected intrusion as established by the administrator so that pre-determined actions take place (e.g, trigger an audible alarm, page or send e-mail to administrator(s), initiate SNMP traps, set up a blind alley, break a network connection, perform special additional auditing, or perform an automatic trace)?	
	Does the product provide at least one 'under attack' administrator alert? (Several types of configurable alert mechanisms are desired; simple screen flashing, e-mail to administrators, and paging alert to administrators.)	
	Does the product give the SA suggested instructions for handling intrusions?	
NCSC-TG-005	Does the product have the ability to react to unauthorized login attempts?	
	Is the reaction to unauthorized login attempts predefined, site configurable, and/or selectable?	

**Table D-5. Access Control Filters Results**

<b>Reference</b>	<b>Operational Requirements</b>	<b>Y / N?</b>
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Does the product support association of filters to a particular interface/port?	
	Does the product perform packet filtering/stateful inspection/proxy on: <ul style="list-style-type: none"> <li>• IP Source Address</li> <li>• IP Destination Addresses</li> <li>• Protocol</li> <li>• TCP Source Port</li> <li>• TCP Destination Port</li> <li>• Source Interface</li> <li>• Destination Interface</li> </ul>	
	Does the product allow combining filters to form an aggregate filter of very narrow focus?	
	Does the product support reconfiguration of the rules set without taking the product out of service?	
	Does the product allow viewing of filters during operation?	
	Does the product provide syntax error checking before implementing an ACL?	
	Does the product provide conflicting rules checking before implementing an ACL?	

**Table D-6. Backup and Redundancy Results**

<b>Reference</b>	<b>Operational Requirements</b>	<b>Y / N?</b>
ISO/IEC 15408-1:19999(E) paragraph 4.3.3 IT Security Requirements	Does the product have the capability to backup and restore the system configuration?	

## APPENDIX E. FEATURES QUESTIONNAIRE

**Table E-1. Additional Features Support**

<b>Test Engineer:</b>		<b>Date (yyymmdd):</b>
Feature	Yes (Y), No (N), or Number Supported	Remarks
<b>Media</b>		
1000Base SX Media (MMF)		
1000Base LX Media (MMF)		
1000Base SX Media (SMF)		
1000Base LH Media (SMF)		
1000Base CX Media (150-Ω STP Copper)		
1000Base T Media (Category 5 UTP)		
<b>Protocols</b>		
OSPF – Equal Cost Multipath		
VRRP Routing Protocol		
OSPF Routing Protocol		
OSPF-OMP Routing Protocol		
BGP4 Routing Protocol		
RIP Routing Protocol		
RIP2 Routing Protocol		
MOSPF		
DVMRP		
PIM-DM		
PIM-SM		
IGMP Version 2		
IGMP Snooping		
IGMP Source Filter		
<b>Redundancy</b>		
Power Supply Redundancy		
Fabric Redundancy		
Processor Redundancy		
<b>Interface</b>		
Drag and Drop VLAN Configuration		
Web Management Interface		
Telnet Management Interface		
Element Manger Interface		
<b>Support</b>		
On Line Help Support		
Tech Support		

**Table E-1. Additional Features Support (continued)**

<b>Number of Edge Device Ethernet Ports</b>		
Stackable 10 Mbps		
Modular Half/Full Duplex 10 Mbps		
Modular 100 Mbps		
Modular Half/Full Duplex 100 Mbps		
Modular 1000 Mbps		
Modular Half/Full Duplex 1000 Mbps		
<b>Layer 3 Switch</b>		
Plug & Play Installation Capability		
Hot-Swappable Modules/Cards		
Number of Slots Supported per Core Device		
Network Interfaces Supported		
Ethernet 10/100 Mbps per Slot		
Gigabit 1000 Mbps per Slot		
<b>Other</b>		
10-Gbps Switch Module		
ASICs IP Version 6 Capable		
Chipset Used?		
Jumbo Frames Supported?		
<b>Quality of Service</b>		
ToS Supported		
Diffserv Supported		
MPLS Supported		
<b>Comments:</b>		

## APPENDIX F. VENDOR INFORMATION

### F-1.0 DEVICE UNDER TEST (DUT) REQUIREMENT

Table F-1 identifies the number of devices required from each vendor for this evaluation. This evaluation only addresses single-vendor solutions. The four evaluation categories are performed concurrently to keep test time to a minimum. Vendors must submit the minimum number of devices in order to participate in this evaluation. Due to time constraints we request vendors submit only one type of core switch, one chassis-based edge device and one stackable edge devices.

**Table F-1. Device Requirements**

<b>Evaluation Category</b>	<b>Remarks</b>	<b>Core Switch Qty</b>	<b>Building Switch Qty</b>	<b>Edge Device Qty</b>
Performance	<ul style="list-style-type: none"> <li>- Two edge devices are required for the Performance portion of the evaluation. Each building switch will have a minimum of twenty-four 10/100-Mbps ports and six 1-gigabit SX ports per device. Each end-user edge device will have a minimum of twenty four 10/100-Mbps ports and two 1-gigabit SX ports per device.</li> <li>- Two core switches are required for the Performance portion of the evaluation. One core switch will have a minimum of forty-eight 10/100-Mbps ports distributed across two blades, and six 1-gigabit SX ports. The second core switch will have a minimum of sixty-four 1-gigabit SX ports.</li> </ul>	2	1	2
System Functionality	<ul style="list-style-type: none"> <li>- Six edge devices are required for the System Functionality portion of the evaluation. Each edge device will have a minimum of twenty-four 10/100-Mbps ports and two 1-gigabit SX ports.</li> <li>- Four core switches are required for the System Functionality portion of the evaluation. Each core switch will have a minimum of eight 1-gigabit SX ports and dual fabric / processor / power supply.</li> </ul>	4	2	6
Network Management	- The Network Management portion of the evaluation will use the System Functionality test network. No additional core switches or edge devices are required for this evaluation category. A complete management software package capable of managing all the above devices including VLAN configuration support is required.	N/A	N/A	N/A
Security	- One core switch and one edge device are required for the Security portion of the evaluation. Security level tests require a minimum of twenty-four 10/100-Mbps ports.	1	1	1

<b>Total Devices Required from Vendor</b>	7	4	9
---	---	---	---

## F-2.0 DEVICE TYPES

Not all tests are performed on every DUT. Table F-2 shows what tests are performed for each device type. Core switches support at least 64 Gigabit Ethernet (GbE) ports. Building switches must support layer 3 and provide at least 6 GbE ports and 24 Fast Ethernet ports. End user edge devices support at least 2 GbE ports and 24 Fast Ethernet (FE) ports.

**Table F-2. Tests Performed on Each Device**

<b>Test Ref</b>	<b>Test Name</b>	<b>Core Switch</b>	<b>Building Switch</b>	<b>End User Edge Device</b>
2.1.1	Single Edge Forwarding		√	√
2.1.2	Single Edge Interframe Gap (IFG)		√	√
2.1.3	Single Edge Congestion Control		√	√
2.1.4	Single Edge Error Filtering		√	√
2.1.5	Single Edge Address Caching		√	√
2.1.6	Single Edge Port Mirroring		√	√
2.1.7	Edge Link Aggregation (Trunking)		√	
2.1.8	Edge 8-Port GbE Throughput		√	
2.2.1	Core 64-Port Performance	√		
2.2.2	Core Interframe Gap (IFG)	√		
2.2.3	Core Congestion Control	√		
2.2.4	Core Error Filtering	√		
2.2.5	Core Address Caching	√		
2.2.6	Core Port Mirroring	√		
2.2.7	Core Link Aggregation	√		
2.2.8	Core Quality of Service (QoS)	√		
2.2.9	Core Multicast Performance	√		
2.2.10	Core 10/100-Port Performance	√	√	
2.3.1	Bridging	√	√	√
2.3.2	Broadcast Distribution and Leak	√	√	√
2.3.3	Edge Routing	√	√	
2.3.4	VLAN Tagging - Bridging and Routing	√	√	√
2.3.5	Multicast Performance	√	√	√
3.2.1	FTP Series	√	√	√
3.2.2	Overnight	√	√	√
3.2.3	Network Recovery	√	√	√
3.2.4	Multicast Streams	√	√	√
3.2.5	Multicast Channel Surfing	√	√	√
3.2.6	Multicast One-to-Many	√	√	√
4.2.1	SNMP Telnet – NT, Solaris, Linux	√	√	√

Test Ref	Test Name	Core Switch	Building Switch	End User Edge Device
4.2.2	SNMP MIB Walk	√	√	√

**Table F-2. Tests Performed on Each Device (continued)**

Test Ref	Test Name	Core Switch	Building Switch	End User Edge Device
4.2.3	SNMP SET/GET Requests	√	√	√
4.2.4	SNMP Traps	√	√	√
4.2.5	SNMP Security	√	√	√
4.2.6	Network Element Configuration	√	√	
4.2.7	Port VLAN Identifier	√	√	
4.2.8	Device Performance Monitoring	√	√	
4.2.9	Network VLAN Configuration	√	√	
5.2.1	Audit Capability	√	√	√
5.2.2	Configuration Management with Secure Remote Management	√	√	√
5.2.3	Product Integrity and Assurance	√	√	√
5.2.4	Network Based Attack Detection	√	√	√
5.2.5	Access Control Filters	√	√	√
5.2.6	Backup and Redundancy	√	√	√

**F-3.0 TEST ADMINISTRATION**

Many vendors have multiple edge device solutions that cannot be evaluated simply due to time constraints. As more vendors enter the layer 3 switch market the problem gets worse. In an effort to identify more devices that meet the CUITN requirement “like” devices may be evaluated using a subset of the complete evaluation. This like device evaluation is only for edge devices when a vendor claims an edge device is similar to an edge device that has successfully completed the layer 3 evaluation. The TIC will determine if the edge device is “like” by comparing hardware, code, and performance in a reduced set of tests. Vendors will be asked for two edge devices for this like device evaluation.

**F-4.0 TEST ADMINISTRATION**

To be recommended for use at CUITN sites each device must pass all priority 1 and 2 tests. If test time becomes a problem the TIC test director may elect not to perform priority 4 and 5 tests. Vendor equipment will be added to a recommended list once it successfully completes the evaluation. Equipment will be dropped from the list 12 months later unless the equipment is successfully re-evaluated within that time.

**F-4.1 Contact Information**

TIC Test Director: Mark Beattie, (520) 533-2807, [BeattieM@hqisec.army.mil](mailto:BeattieM@hqisec.army.mil)

Layer 3 Lead Test Engineer: Mark McFadden, (520) 533-2817, [McfaddenM@hqisec.army.mil](mailto:McfaddenM@hqisec.army.mil)

#### **F-4.2 Shipping Address**

The shipping address for equipment to be tested is as follows:

Commander, USAISEC  
Technology Integration Center  
ATTN: AMSEL-IE-TI (Mark McFadden)  
Building 53302  
Fort Huachuca, AZ 85613-5300  
(520) 533-2690

#### **F-4.3 Laboratory Access**

Normal laboratory hours are from 0800 to 1700 hours, Monday through Friday, excluding holidays. Under TIC supervision, vendors are permitted onsite during the evaluation and are expected to perform the setup and configuration of their products.

#### **F-4.4 Vendor Guidelines**

Vendors considered for product evaluation will be notified and provided a copy of this test plan and their proposed test schedule. The TIC must receive vendor responses no later than the specified response cutoff date. Equipment is tested as submitted; code and equipment revisions or substitutions are not permitted once testing begins. All equipment evaluated must be commercially available for purchase on the date tested. Beta versions of code or hardware are not permitted. Vendors are expected to provide the TIC with the following items no later than 1 week prior to the beginning of the scheduled test period:

- a. A technical point of contact available for support and assistance during the evaluation.
- b. Current documentation or detailed instructions concerning the setup, configuration, and operation for each device submitted.
- c. An itemized list of all equipment submitted for test. This listing must include (as applicable) the model name/number, serial number, hardware version, firmware version, software version, and number of units for each chassis and plug-in processing and interface card/module submitted for test.

#### **F-5.0 EVALUATION PLAN REVISIONS**

The TIC reserves the right to modify this evaluation plan at any time.



## APPENDIX G. SMARTBITS CONFIGURATION

The main test equipment used for the performance portion of this evaluation plan is Spirent Communications SmartBits network performance analyzer. The following sections describe the SmartBits software and hardware that is used for the layer 3 evaluations.

### G-1.0 APPLICATIONS

The following SmartBits applications are used in the performance portion of the evaluation.

a. **Advanced Switch Tests (AST):** Version 2.10. AST is Spirent Communications' first generation of Advanced Switch tests.

b. **Advanced Switch Tests II (AST II):** Version 2.00. AST II is Spirent Communications' second generation of Advanced Switch tests. Based on RFC 2285 and the IETF Switch Methodology Draft, AST II provides the TRUE first-level benchmark for all switches. AST II tests include Forwarding, Congestion Control, Address Learning Rate, Address Caching, Error Filtering, Broadcast Forwarding, Broadcast Latency, and Forward Pressure.

c. **SmartMulticastIP:** Version 1.26. Measures IP multicast performance of routers and switches. Designed for network managers, network equipment manufacturers, ISPs, and carriers. Used to perform a comparative analysis of IP multicast devices, to evaluate key performance parameters of IP multicast devices under typical or extreme traffic load conditions, and to re-qualify IP multicast devices after firmware upgrades.

d. **SmartWindow:** Version 7.20. SmartBits™ virtual front panel. Allows the user to access SmartBits™ equipment with greater test control than a pre-programmed application. Used to verify design, improve product quality, perform low-volume production and repair testing, and perform competitive marketing analysis. Within SmartWindow, simply select a protocol, set class of service parameters, and then test any of the following: NIC cards, servers, bridges, cable modems, xDSL modems, switches, routers, VLANs, firewalls, live networks, or multimedia scenarios.

e. **SmartFlow:** Version 1.33. Tests line rate QoS. Enables both forwarding and policy tests. Analyzes each incoming stream to test a device's (or network's) ability to forward very large numbers of flows. Analyzes the device's ability to correctly handle policies implemented in the network or device under test.

### G-2.0 TERMS

The following descriptions explain how common terms are defined when using SmartFlow.

a. **Throughput:** The Throughput test determines the maximum transmission rate at which the DUT can forward IP traffic with no frame loss, or at a user-specified acceptable frame loss. By increasing the transmission rate at specified levels you can determine the DUT's capacity. SmartFlow calculates frame loss as:

$$\text{Frame Loss} = \text{Number of Frames Transmitted} - \text{Number of Frames Received}$$

b. **Frame Loss:** The Frame Loss test measures the percentage of frames lost by the DUT that should have been forwarded. This test is used to determine a DUT's ability to deliver frames in a sequenced flow of streams with specific routing priorities and at a stepped percentage of the wire rate.

Frame Loss = Number of Frames Transmitted - Number of Frames Received

c. **Latency Test:** The Latency test is used to measure latency above and below the load percentage at which the DUT drops frames. It calculates the minimum, maximum and average latency at different loads. Latency is defined as the length of time it takes a DUT to forward a packet from one SmartBits port to another SmartBits port. The Latency test measures latency for received frames only.

Latency = Receive Timestamp - Transmit Timestamp

d. **Latency Distribution Test:** The Latency Distribution test measures the latency of each frame on a frame-by-frame basis and places latency results into eight time buckets. SmartFlow reads the time the sending SmartBits port sent the frame (Transmit Timestamp) and the time the receiving SmartBits recognizes the trigger frame, which is the Receive Timestamp. This test uses the specified test duration, a starting percentage load (based on the wire rate), a step percentage by which to increase the load during the test, and a stop percentage at which the test ends. During the test, these three values determine the duration for which the DUT is tested at a specified load. Note: Latency values are for the frames that were not dropped.

Latency = Receive Timestamp - Transmit Timestamp

e. **Jumbo Test:** The Jumbo test is a combination of the Latency, Latency Distribution and Frame Loss tests. It also measures latency variation (standard deviation) in addition to frame loss, latency, latency distribution, and sequencing. Note: The Jumbo test updates all types of results in each test (except Latency Snapshot and Throughput) simultaneously.

### G-3.0 HARDWARE

Table G-1 lists the SmartBits hardware used in the lab. There are six SMB 6000B chassis fully loaded with 12 each 3201A GbE modules. There are four SMB 2000 chassis fully loaded with 10/100 and GbE modules.

**Table G-1. SmartBits Hardware**

Device Model/Name	Hardware Version	Software Version	Remarks
SmartBits 6000B	SMB 6000B	1.07.009	
SmartBits LAN-3201A Gigabit Ethernet Module	LAN-3201A	2.02.009	Also known as the LAN-6201A
SmartBits 2000 Chassis	SMB 2000	6.67.001	
SmartBits ML-7710 SmartMetrics Card	ML-7710	2.20.011	
SmartBits GX-1405B Gigabit Ethernet Card	GX-1405B	2.30.01	

## **APPENDIX H. SYSTEM FUNCTIONALITY TEST CONFIGURATION**

### **H-1.0 NETWORK PERFORMANCE TOOLS**

There are two ways to generate traffic over the test network, using remote terminal emulations (RTEs) or using Chariot.

#### **H-1.1 RTE**

The RTE is the primary means for this integrated system test. It is a combination hardware/software platform consisting of Intel Pentium-based personal computers (PCs) running the Red Hat Linux operating system and specialized application software developed by Neal Nelson and Associates. This platform makes practical the capability to mimic thousands of typical Internet junkies exchanging real world information with each other and pulling files from the built in Linux Apache file servers. The RTE logs the results of these tests as transaction completion counts and time statistics. At the end of the test, the RTE performs post processing of the logs and generates customized reports designed for the specific evaluation. The RTE has many capabilities that are not used in this evaluation.

The RTE generates File Transfer Protocol (FTP) Puts, FTP Gets, worldwide web (WWW), Telnet, rlogin, multicast streaming, and Simple Mail Transfer Protocol (SMTP) traffic for the test network. The only non-test traffic placed on the test network is usually Simple Network Management Protocol (SNMP), ping, and trace-routes which are for troubleshooting and are not significant enough to skew the test results to any noticeable degree due to the granularity set for the test data accumulation. There are 72 Ethernet connections from 36 RTE computers to the test network edge devices, with the two network interface card (NIC) connections on each computer labeled as B-local area network (LAN) and C-LAN. Both are fixed at 100 megabits per second (Mbps), full duplex to help avoid hardware interface issues. Static routing is programmed into the RTEs in order to control and track the traffic on each NIC. In the unicast traffic programs, the simulated users are evenly distributed across the RTE computers. Most of the unicast tests consist of 70 users per computer across 36 computers for a total of 2,520 functionally identical users that exchange traffic with each other and/or with the 36 Apache servers (across 36 computers). The RTE test traffic programs are set to run in tight loops with essentially no "think delays" between transaction commands.

#### **H-1.2 Chariot**

Secondary testing is also performed using the commercially proven Chariot network performance tool from NetIQ (formally Ganymede). Like the RTE, this tool simulates real world traffic using a specialized application program called an endpoint. The endpoint software resides on all computers that are designated to generate test traffic under the control of the Chariot console. The endpoint software is a layer 7 (L7) application that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) stack within the hardware/operating system platform for which it is installed. The RTE computers are used as the endpoint stations and are dual bootable to either the Linux or Windows 2000 Server operating system for which the endpoint program can reside. The computers can be loaded with any mixture of Linux and Windows 2000 combinations as the Chariot Console makes no differentiation except to capture information on the particular operating system that each of its endpoints are operating under for logging purposes. The endpoint software has the capability to stuff its packets with compressible and non-compressible patterns, canned and

customized test files that Chariot can use to compare for bit integrity. The Chariot scripts written for this evaluation are similar to but generally shorter in duration than the RTE test programs and are generally performed as needed to provide a “second opinion.” The Chariot Console computer coordinates and receives statistics from the endpoints through an administration network that is independent of the test network. This eliminates having to use the test network to transfer the endpoints statistics to the Chariot Console for evaluation because it would interfere with the tests.

## **H-2.0 NETWORK CONFIGURATION**

Figures H-1 through H-3 show the System Functionality test network. This test network models the Common User Installation Transport Network (CUITN) without lateral links between area distribution nodes (ADNs). These lateral links were removed in the test network to increase traffic through the main control nodes (MCNs) without modifying open shortest path first (OSPF) cost on each link. The top-down architecture of the CUITN network is segregated into three physical tiers as shown on the left side of the figures. Tier 3 consists of the backbone system where most L3 inter-installation traffic and incoming/outgoing Internet traffic is switched or routed with full redundancy. Tier 2 is an L2 and L3 hybrid that handles most of the end-user building (EUB) link redundancy and augments the backbone for inter-installation traffic. Tier 1 is also L2 and L3 capable and consists of the installation tenants and EUB devices.

Two logical networks, a 6-subnet (Figures H-1 and H-2) using an untagged VLAN network and a 6-VLAN (Figure H-3) using VLAN tagging, are individually tested against identical physical architectures. The ADNs and MCNs are referred to as the core of the network. In both logical networks, the ADNs are the gateway for each VLAN or subnet. It can be assumed that the link between the two MCNs normally serves no function other than to act as a backup in case the MCN A to ADN 2 link and the MCN B to ADN 1 links both fail. The test network conforms to the following parameters for all of the tests in this appendix regardless of whether or not they are a function of a particular test:

- OSPF routing
- OSPF equal-cost multi-path (generally applies to 6-subnet only)
- PIM-DM (preferred) or DVMRP
- OSPF area set to anything other than 0
- Passwords are not necessary
- Telnet access is activated on all devices
- VLANs are implemented with 802.1Q
- PIM is assigned to all core links if possible
- IGMP version 2 snooping is enabled on edge devices
- Untagged VLANs (if used) on all end user ports
- Spanning tree disabled where possible
- No flow control on any port
- End user ports are fixed at 100 Mbps, full duplex

- The defined Gateway IP addresses must be used
- No QOS structures defined
- No proprietary “tweaks” are allowed; tuning for performance is okay

The IP address scheme for the RTE to edge device connections is located in Table H-1.

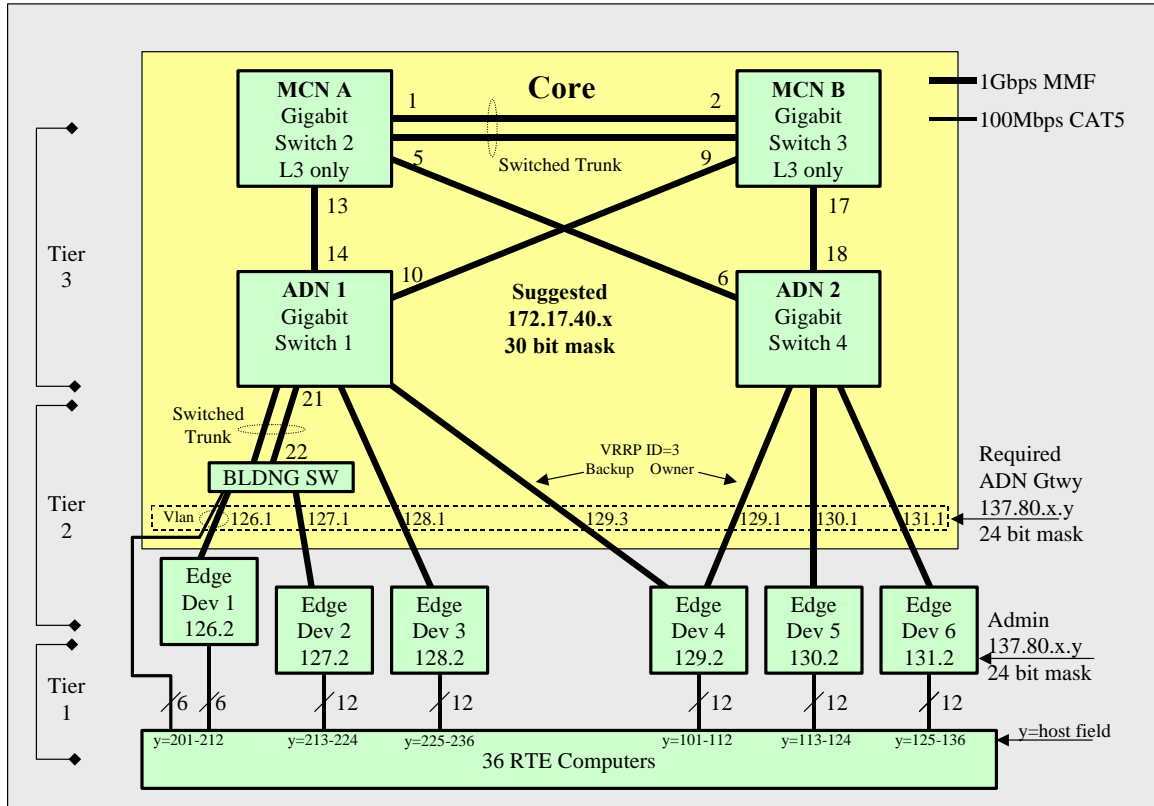
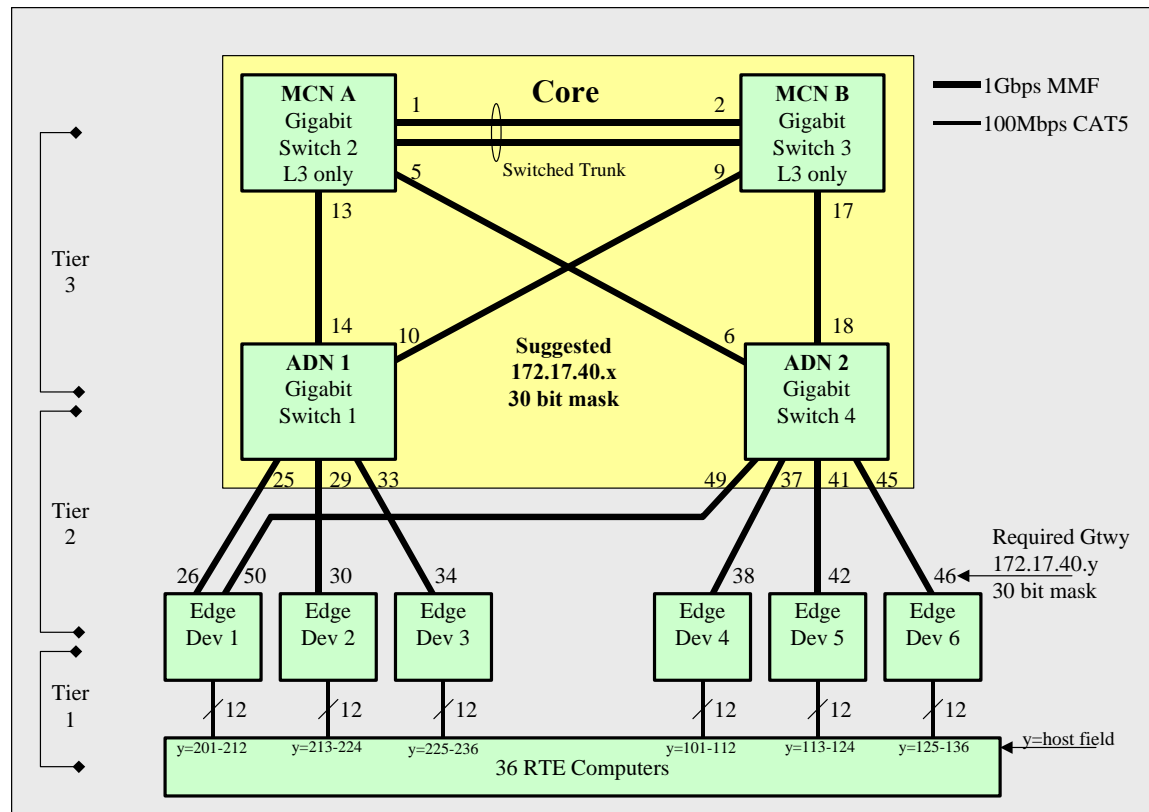


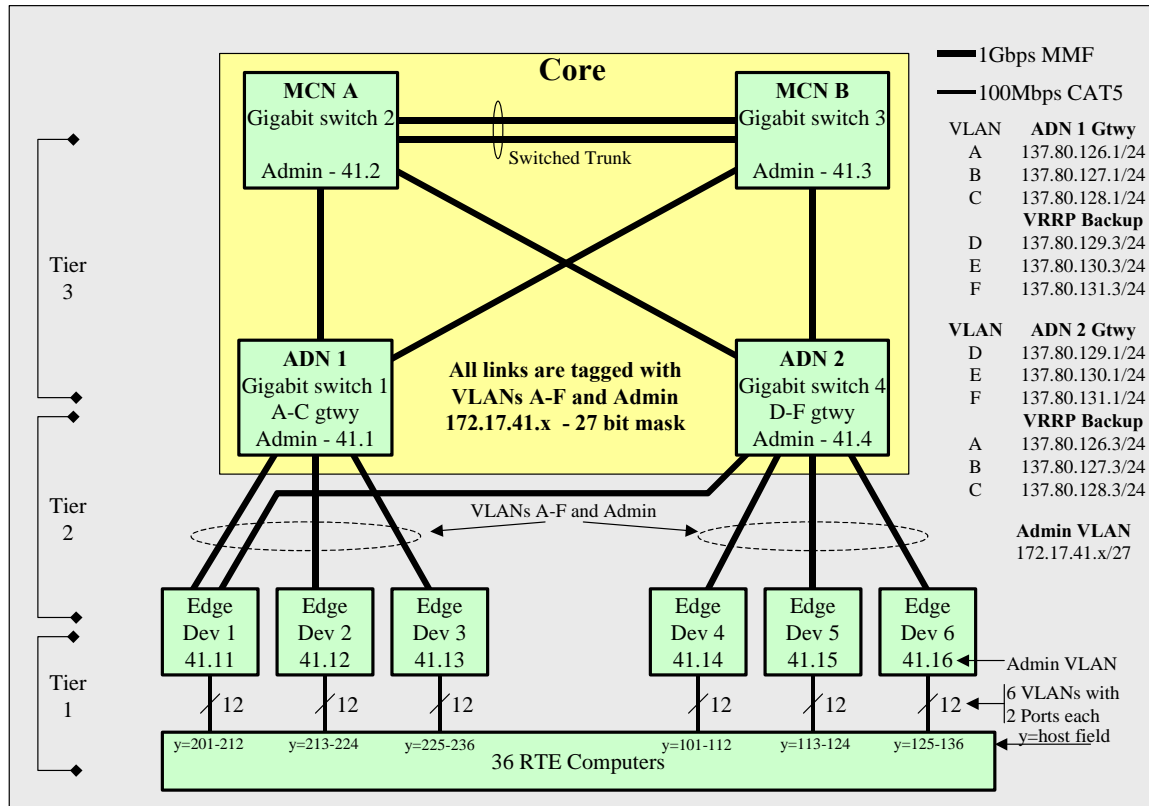
Figure H-1. 6-Subnet Configuration with L2 at Tier 1



**Figure H-2. 6-Subnet Configuration with L3 at Tier 1**

### H-2.1 6-Subnet

This is a flat VLAN architecture network that follows the physical network architecture where each of the six edge devices is entirely in its own subnet. This test is designed to show basic unicast and multicast functions of the vendor equipment used in a straightforward design and is usually the first test conducted. This test has two iterations which Figures H-1 and H-2 illustrate. In Figure H-1 the ADNs act as the L3 gateway for each edge device, while in Figure H-2, if possible, the edge devices become the L3 gateways. In both iterations, the L3 routing allows spanning tree protocol to be deactivated and OSPF equal cost multi-path provides the necessary core device and link redundancy. Although this is not a performance test, the network allows some of the RTE test programs to run at its maximum rate while other tests are regulated to operate at a specific rate. The results of these tests are then compared to a baseline that has been established as a reference. The test is evaluated through this comparison in conjunction with a consistent traffic flow and equal service with all users.



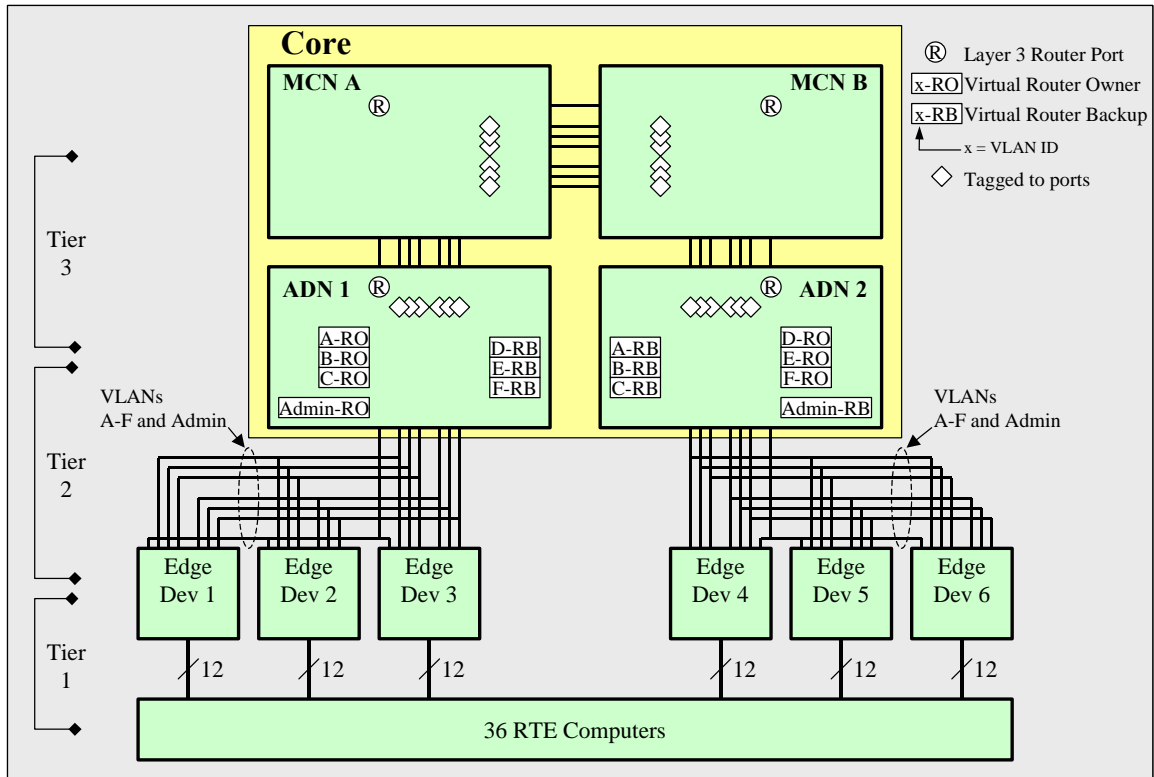
**Figure H-3. 6-VLAN Configuration and VLAN Logical Flow**

## H-2.2 6-VLAN

This configuration is designed to stress tagged VLANs and L3 functionality by routing packets multiple times through the core with L3 routing function redundancy on all VLANs. This is not a performance test so throughput is not an issue. Rather, this test evaluates the robustness of L2 VLAN tagging and L3 routing functions of the core and edge devices. Spanning tree protocol generally is activated throughout the core links to prevent L2 traffic loops. The test results are not generally compared to any baseline as such, but are analyzed mainly for consistent throughput and equal service for all sessions, indicating functionality and reliance.

Six broadcast domains (RTE test VLANs) and an administration domain all appear at every edge device through the core using VLAN tagging. Figure H-4 is a logical diagram illustrating this concept; Figure H-3 shows how the VLANs map onto the physical network. With the RTE test VLAN L3 gateways located in the ADNs, the core is forced to route packets across the individual core links as many as three times (L21 - L3 - L22 - L3 - L23) before it reaches its destination. Generally, the preferred configuration of the gateways is such that each ADN owns four of the gateways and acts as backup for the other four gateways that are owned by the other ADN, which Figure H-4 illustrates. The ADNs act as backups for each other in case one of them fails. As a less preferred alternative, one ADN can own all eight gateways while the other acts as backup. Regardless of how the gateways are configured, the ADNs still provide L2 redundancy to the edge devices, which is demonstrated by the first edge device with its dual-homed links. It is assumed that the remaining edge devices will function in the same manner as the first if they also had

redundant links. All edge devices are programmed identically with the exception of the unique administration host IP address for the administration VLAN. At each edge device, with 12 Ethernet ports labeled as 1 through 12, port 1 and 7 are assigned untagged to the first RTE test VLAN, ports 2 and 8 to the second, and so on through the sixth.



**Figure H-4. 6-VLAN Logical Connections**

The redundancy method used between the ADNs is usually implemented using an RFC standard such as Virtual Router Redundancy Protocol (VRRP); however, vendor specific solutions may be implemented if VRRP is not possible in the interest of showing progression towards using an RFC standard. The three VLANs, G, H, and I, provide L3 connectivity throughout the core for the six gateways while the Admin VLAN provides an independent management network. Spanning tree is turned on throughout the core and edge devices on all 10 VLANs to prevent L2 traffic loops. If possible, spanning tree priorities are implemented so that the four gateways assigned to each ADN has the best route to all edge devices. This is the suggested method to implementing L2 and L3 connectivity but can be implemented in some other method at the vendor's discretion.

### H-2.3 Fail-over and Recovery

The fail-over implementation is such that any one link or MCN can fail without causing loss of core network access to any host. Also, a loss of an ADN does not deny core network access to any host of the remaining ADN. Although throughput performance is not a factor in this evaluation, the vendor is encouraged to load share traffic across the core links. It is more important, however, to maintain fail-over capability. In addition, the network manager must be able to Telnet to and manage all devices in this network at all times upon network fail-over states, recoveries, and during non-congestive traffic.



## H-2.4 IP addressing Scheme

The following tables show the IP addressing scheme used in the System Functionality test network.

**Table H-1. RTE 201-236 IP Addressing 6-Subnet**

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	VLAN	Cable	Edge
s201b	137.80.126.101	Dflt	1	1-01	s201c	137.80.129.201	Dflt	37	4-12
s202c	137.80.126.102	Dflt	38	1-01	s202b	137.80.129.202	Dflt	2	4-11
s203b	137.80.126.103	Dflt	3	1-03	s203c	137.80.129.203	Dflt	39	4-10
s204c	137.80.126.104	Dflt	40	1-04	s204b	137.80.129.204	Dflt	4	4-09
s205b	137.80.126.105	Dflt	5	1-05	s205c	137.80.129.205	Dflt	41	4-08
s206c	137.80.126.106	Dflt	42	1-06	s206b	137.80.129.206	Dflt	6	4-07
s207b	137.80.126.107	Dflt	7	1-07	s207c	137.80.129.212	Dflt	43	4-06
s208c	137.80.126.108	Dflt	44	1-08	s208b	137.80.129.211	Dflt	8	4-05
s209b	137.80.126.109	Dflt	9	1-09	s209c	137.80.129.210	Dflt	45	4-04
s210c	137.80.126.110	Dflt	46	1-10	s210b	137.80.129.209	Dflt	10	4-03
s211b	137.80.126.111	Dflt	11	1-11	s211c	137.80.129.208	Dflt	47	4-02
s212c	137.80.126.112	Dflt	48	1-12	s212b	137.80.129.207	Dflt	12	4-01
s213b	137.80.127.113	Dflt	13	2-01	s213c	137.80.130.213	Dflt	49	5-12
s214c	137.80.127.114	Dflt	50	2-01	s214b	137.80.130.214	Dflt	14	5-11
s215b	137.80.127.115	Dflt	15	2-03	s215c	137.80.130.215	Dflt	51	5-10
s216c	137.80.127.116	Dflt	52	2-04	s216b	137.80.130.216	Dflt	16	5-09
s217b	137.80.127.117	Dflt	17	2-05	s217c	137.80.130.217	Dflt	53	5-08
s218c	137.80.127.118	Dflt	54	2-06	s218b	137.80.130.218	Dflt	18	5-07
s219b	137.80.127.119	Dflt	19	2-07	s219c	137.80.130.224	Dflt	55	5-06
s220c	137.80.127.120	Dflt	56	2-08	s220b	137.80.130.223	Dflt	20	5-05
s221b	137.80.127.121	Dflt	21	2-09	s221c	137.80.130.222	Dflt	57	5-04
s222c	137.80.127.122	Dflt	58	2-10	s222b	137.80.130.221	Dflt	22	5-03
s223b	137.80.127.123	Dflt	23	2-11	s223c	137.80.130.220	Dflt	59	5-02
s224c	137.80.127.124	Dflt	60	2-12	s224b	137.80.130.219	Dflt	24	5-01
s225b	137.80.128.125	Dflt	25	3-01	s225c	137.80.131.225	Dflt	61	6-12
s226c	137.80.128.126	Dflt	62	3-01	s226b	137.80.131.226	Dflt	26	6-11
s227b	137.80.128.127	Dflt	27	3-03	s227c	137.80.131.227	Dflt	63	6-10
s228c	137.80.128.128	Dflt	64	3-04	s228b	137.80.131.228	Dflt	28	6-09
s229b	137.80.128.129	Dflt	29	3-05	s229c	137.80.131.229	Dflt	65	6-08
s230c	137.80.128.130	Dflt	66	3-06	s230b	137.80.131.230	Dflt	30	6-07
s231b	137.80.128.131	Dflt	31	3-07	s231c	137.80.131.236	Dflt	67	6-06
s232c	137.80.128.132	Dflt	68	3-08	s232b	137.80.131.235	Dflt	32	6-05
s233b	137.80.128.133	Dflt	33	3-09	s233c	137.80.131.234	Dflt	69	6-04
s234c	137.80.128.134	Dflt	70	3-10	s234b	137.80.131.233	Dflt	34	6-03
s235b	137.80.128.125	Dflt	35	3-11	s235c	137.80.131.232	Dflt	71	6-02
s236c	137.80.128.136	Dflt	72	3-12	s236b	137.80.131.231	Dflt	36	6-01

**Table H-2. RTE 201-236 IP Addressing 6-VLAN**

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	VLAN	Cable	Edge
s201b	137.80.126.101	2	1	1-01	s201c	137.80.131.201	7	37	4-12
s202c	137.80.127.102	3	38	1-01	s202b	137.80.130.202	6	2	4-11
s203b	137.80.128.103	4	3	1-03	s203c	137.80.129.203	5	39	4-10
s204c	137.80.129.104	5	40	1-04	s204b	137.80.128.204	4	4	4-09
s205b	137.80.130.105	6	5	1-05	s205c	137.80.127.205	3	41	4-08
s206c	137.80.131.106	7	42	1-06	s206b	137.80.126.206	2	6	4-07
s207b	137.80.126.107	2	7	1-07	s207c	137.80.131.207	7	43	4-06
s208c	137.80.127.108	3	44	1-08	s208b	137.80.130.208	6	8	4-05
s209b	137.80.128.109	4	9	1-09	s209c	137.80.129.209	5	45	4-04
s210c	137.80.129.110	5	46	1-10	s210b	137.80.128.210	4	10	4-03
s211b	137.80.130.111	6	11	1-11	s211c	137.80.127.211	3	47	4-02
s212c	137.80.131.112	7	48	1-12	s212b	137.80.126.212	2	12	4-01
s213b	137.80.126.113	2	13	2-01	s213c	137.80.131.213	7	49	5-12
s214c	137.80.127.114	3	50	2-01	s214b	137.80.130.214	6	14	5-11
s215b	137.80.128.115	4	15	2-03	s215c	137.80.129.215	5	51	5-10
s216c	137.80.129.116	5	52	2-04	s216b	137.80.128.216	4	16	5-09
s217b	137.80.130.117	6	17	2-05	s217c	137.80.127.217	3	53	5-08
s218c	137.80.131.118	7	54	2-06	s218b	137.80.126.218	2	18	5-07
s219b	137.80.126.119	2	19	2-07	s219c	137.80.131.219	7	55	5-06
s220c	137.80.127.120	3	56	2-08	s220b	137.80.130.220	6	20	5-05
s221b	137.80.128.121	4	21	2-09	s221c	137.80.129.221	5	57	5-04
s222c	137.80.129.122	5	58	2-10	s222b	137.80.128.222	4	22	5-03
s223b	137.80.130.123	6	23	2-11	s223c	137.80.127.223	3	59	5-02
s224c	137.80.131.124	7	60	2-12	s224b	137.80.126.224	2	24	5-01
s225b	137.80.126.125	2	25	3-01	s225c	137.80.131.225	7	61	6-12
s226c	137.80.127.126	3	62	3-01	s226b	137.80.130.226	6	26	6-11
s227b	137.80.128.127	4	27	3-03	s227c	137.80.129.227	5	63	6-10
s228c	137.80.129.128	5	64	3-04	s228b	137.80.128.228	4	28	6-09
s229b	137.80.130.129	6	29	3-05	s229c	137.80.127.229	3	65	6-08
s230c	137.80.131.130	7	66	3-06	s230b	137.80.126.230	2	30	6-07
s231b	137.80.126.131	2	31	3-07	s231c	137.80.131.231	7	67	6-06
s232c	137.80.127.132	3	68	3-08	s232b	137.80.130.232	6	32	6-05
s233b	137.80.128.133	4	33	3-09	s233c	137.80.129.233	5	69	6-04
s234c	137.80.129.134	5	70	3-10	s234b	137.80.128.234	4	34	6-03
s235b	137.80.130.125	6	35	3-11	s235c	137.80.127.235	3	71	6-02
s236c	137.80.131.136	7	72	3-12	s236b	137.80.126.236	2	36	6-01

**Table H-3. RTE 201-236 IP Addressing 36-Subnet**

RTE	IP Address	VLAN	Cable	Edge	RTE	IP Address	VLAN	Cable	Edge
s201b	137.80.126.101	2	1	1-01	s201c	137.80.144.101		37	4-12
s202c	137.80.127.102	3	38	1-01	s202b	137.80.145.102		2	4-11
s203b	137.80.128.103	4	3	1-03	s203c	137.80.146.103		39	4-10
s204c	137.80.129.104	5	40	1-04	s204b	137.80.147.104		4	4-09
s205b	137.80.130.105	6	5	1-05	s205c	137.80.148.105		41	4-08
s206c	137.80.131.106	7	42	1-06	s206b	137.80.149.106		6	4-07
s207b	137.80.131.107	7	7	1-07	s207c	137.80.149.112		43	4-06
s208c	137.80.130.108	6	44	1-08	s208b	137.80.148.111		8	4-05
s209b	137.80.129.109	5	9	1-09	s209c	137.80.147.110		45	4-04
s210c	137.80.128.110	4	46	1-10	s210b	137.80.146.109		10	4-03
s211b	137.80.127.111	3	11	1-11	s211c	137.80.145.108		47	4-02
s212c	137.80.126.112	2	48	1-12	s212b	137.80.144.107		12	4-01
s213b	137.80.132.113	8	13	2-01	s213c	137.80.150.113		49	5-12
s214c	137.80.132.114	8	50	2-01	s214b	137.80.150.114		14	5-11
s215b	137.80.133.115	9	15	2-03	s215c	137.80.151.115		51	5-10
s216c	137.80.133.116	9	52	2-04	s216b	137.80.151.116		16	5-09
s217b	137.80.134.117	10	17	2-05	s217c	137.80.152.117		53	5-08
s218c	137.80.134.118	10	54	2-06	s218b	137.80.152.118		18	5-07
s219b	137.80.135.119	11	19	2-07	s219c	137.80.153.124		55	5-06
s220c	137.80.135.120	11	56	2-08	s220b	137.80.153.123		20	5-05
s221b	137.80.136.121	12	21	2-09	s221c	137.80.154.122		57	5-04
s222c	137.80.136.122	12	58	2-10	s222b	137.80.154.121		22	5-03
s223b	137.80.137.123	13	23	2-11	s223c	137.80.155.120		59	5-02
s224c	137.80.137.124	13	60	2-12	s224b	137.80.155.119		24	5-01
s225b	137.80.138.125	14	25	3-01	s225c	137.80.156.125		61	6-12
s226c	137.80.141.126	17	62	3-01	s226b	137.80.159.126		26	6-11
s227b	137.80.138.127	14	27	3-03	s227c	137.80.156.127		63	6-10
s228c	137.80.141.128	17	64	3-04	s228b	137.80.159.128		28	6-09
s229b	137.80.139.129	15	29	3-05	s229c	137.80.157.129		65	6-08
s230c	137.80.142.130	18	66	3-06	s230b	137.80.160.130		30	6-07
s231b	137.80.139.131	15	31	3-07	s231c	137.80.157.136		67	6-06
s232c	137.80.142.132	18	68	3-08	s232b	137.80.160.135		32	6-05
s233b	137.80.140.133	16	33	3-09	s233c	137.80.158.134		69	6-04
s234c	137.80.143.134	19	70	3-10	s234b	137.80.161.133		34	6-03
s235b	137.80.140.125	16	35	3-11	s235c	137.80.158.132		71	6-02
s236c	137.80.143.136	19	72	3-12	s236b	137.80.161.131		36	6-01

Table H-4. RTE Multicast Groups

Group #1		Group #2		Group #3		Group #4		Group #5		Group #6	
1	s211a	8	s212a	15	s223a	22	s224a	29	s235a	36	s236a
2	s201a	9	s203a	16	s205a	23	s207a	30	s209a	37	s211a
3	s202a	10	s204a	17	s206a	24	s208a	31	s210a	38	s212a
4	s213a	11	s215a	18	s217a	25	s219a	32	s221a	39	s223a
5	s214a	12	s216a	19	s218a	26	s220a	33	s222a	40	s224a
6	s225a	13	s227a	20	s229a	27	s231a	34	s233a	41	s234a
7	s226a	14	s228a	21	s230a	28	s232a	35	s236a	42	s235a
Group #7		Group #8		Group #9		Group #10		Group #11		Group #12	
43	s201a	50	s202a	57	s213a	64	s214a	71	s225a	78	s226a
44	s203a	51	s205a	58	s207a	65	s209a	72	s211a	79	s201a
45	s204a	52	s206a	59	s208a	66	s210a	73	s212a	80	s202a
46	s213a	53	s215a	60	s217a	67	s219a	74	s221a	81	s223a
47	s214a	54	s216a	61	s218a	68	s220a	75	s222a	82	s224a
48	s225a	55	s227a	62	s229a	69	s231a	76	s233a	83	s235a
49	s226a	56	s228a	63	s230a	70	s232a	77	s234a	84	s236a
Group #13		Group #14		Group #15		Group #16		Group #17		Group #18	
85	s203a	92	s204a	99	s215a	106	s216a	113	s227a	120	s228a
86	s204a	93	s203a	100	s207a	107	s209a	114	s211a	121	s201a
87	s205a	94	s206a	101	s208a	108	s210a	115	s212a	122	s202a
88	s213a	95	s215a	102	s217a	109	s219a	116	s221a	123	s223a
89	s214a	96	s216a	103	s218a	110	s220a	117	s222a	124	s224a
90	s225a	97	s227a	104	s229a	111	s229a	118	s233a	125	s235a
91	s226a	98	s228a	105	s230a	112	s232a	119	s234a	126	s236a
Group #19		Group #20		Group #21		Group #22		Group #23		Group #24	
127	s205a	134	s206a	141	s217a	148	s218a	155	s229a	162	s230a
128	s204a	135	s201a	142	s203a	149	s205a	156	s207a	163	s209a
129	s211a	136	s208a	143	s206a	150	s210a	157	s212a	164	s202a
130	s213a	137	s215a	144	s219a	151	s217a	158	s221a	165	s223a
131	s214a	138	s216a	145	s218a	152	s220a	159	s222a	166	s224a
132	s225a	139	s227a	146	s229a	153	s231a	160	s233a	167	s235a
133	s226a	140	s228a	147	s230a	154	s232a	161	s234a	168	s236a
Group #25		Group #26		Group #27		Group #28		Group #29		Group #30	
169	s207a	176	s208a	183	s221a	190	s222a	197	s231a	204	s232a
170	s204a	177	s201a	184	s203a	191	s205a	198	s207a	205	s202a
171	s211a	178	s206a	185	s204a	192	s210a	199	s212a	206	s209a
172	s213a	179	s215a	186	s217a	193	s219a	200	s221a	207	s223a
173	s214a	180	s216a	187	s218a	194	s220a	201	s222a	208	s224a
174	s225a	181	s227a	188	s229a	195	s231a	202	s233a	209	s235a
175	s226a	182	s228a	189	s230a	196	s232a	203	s234a	210	s236a
Group #31		Group #32		Group #33		Group #34		Group #35		Group #36	
211	s209a	218	s210a	225	s219a	232	s220a	239	s233a	246	s234a
212	s204a	219	s201a	226	s203a	233	s205a	240	s207a	247	s202a
213	s211a	220	s206a	227	s208a	234	s210a	241	s212a	248	s209a
214	s213a	221	s215a	228	s217a	235	s218a	242	s221a	249	s223a
215	s214a	222	s216a	229	s220a	236	s219a	243	s222a	250	s224a
216	s225a	223	s227a	230	s229a	237	s232a	244	s231a	251	s235a
217	s226a	224	s228a	231	s230a	238	s233a	245	s234a	252	s236a

**This page is intentionally left blank.**



**GLOSSARY. ACRONYMS AND ABBREVIATIONS**

ACL	Access Control List
AST	Advanced Switch Test
ATTN	attention
CONUS	continental U.S.
COTS	commercial off-the-shelf
CRC	Cyclic Redundancy Check
CUITN	Common User Installation Transport Network
DREC	Dynamic
DSN	Defense Switched Network
DUT	device under test
FE	Fast Ethernet
fps	frames per second
FTP	File Transfer Protocol
GbE	Gigabit Ethernet
GIF	Graphic Interchange Format
GUI	graphical user interface
HTTP	Hypertext Transfer Protocol
IEEE	Institute for Electrical and Electronics Engineers
IFG	Interframe Gap
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISS	Internet Security Systems
kB	kilobyte
MAC	Medium Access Control
MB	megabyte
Mbps	megabits per second
MCALC	multicast calculator
MCN	main control node
MGEN	Multicast Generator
MIB	Management Information Base
NAI	Network Associates Incorporated
NMS	Network Management Stations
OSPF	open shortest path first

PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PM, DDN	Product Manager, Defense Data Networks
PVID	Port VLAN Identifier
QoS	Quality of Service
RMON	Remote Monitoring
RTE	remote terminal emulation
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	structured query language
TIC	Technology Integration Center
USAISEC	U.S. Army Information Systems Engineering Command
VLAN	virtual local area network
VRRP	Virtual Router Redundancy Protocol
WWW	worldwide web